MAYER·BROWN

Electronic Discovery & Records Management

2011 TIPS OF THE MONTH – A Compilation

Table of Contents

Tip of the Month

Introduction

2011 Trends in E-Discovery

In 2011, we saw the continued evolution of e-discovery, as courts, counsel and clients alike focused on the costs and complexities associated with managing electronically stored information (ESI). Key issues included the increasing recognition of the cross-disciplinary nature of e-discovery, a continued emphasis on cooperation, revisions to the discovery rules impacting ESI, the discoverability of social media, the obligations of the US government when it comes to e-discovery, and prevailing parties seeking to recover e-discovery costs.

E-Discovery and Information Governance
Organizations increasingly realized that e-discovery is about more than just litigation: that it has wide-reaching implications across an entire organization. In truth, organizations are struggling with not just e-discovery, but with information governance itself: how an organization stores, manages, monitors, tracks and protects its electronic data. In coming to terms with this reality, many organizations launched organization-wide initiatives that brought together personnel from management, legal, information technology, records management, procurement, human resources and data privacy in order to create comprehensive data management programs that control costs, improve business efficiency, and protect against legal risks.

Cooperation in E-Discovery
Despite hopes from many litigants (and lawyers) that the courts' nearly uniform adoption of The Sedona Conference's® *Cooperation Proclamation* would wane in 2011, courts continued to press litigation counsel to cooperate in resolving e-discovery disputes.[i] Litigants should expect that trend to continue, and start searching for better and more effective ways to negotiate solutions to e-discovery disputes with opposing counsel.

Reforming the E-Discovery Rules
State and federal courts across the country explored ways to update their e-discovery practices. For example, the Federal Rules Committee began evaluating potential amendments to the Federal Rules of Civil Procedure to address preservation concerns, the Southern District of New York launched a pilot program for complex cases designed to improve the judicial case management of complex civil cases, including provisions specifically relating to e-discovery,[ii] and the Federal Circuit Advisory Counsel adopted a model order governing e-discovery in patent litigations.[iii]

In addition, several state courts considered or promulgated e-discovery rules in 2011, including the Delaware Chancery Court,[iv] North Carolina[v] and the Supreme Court of Pennsylvania.[vi] Expect further discussion on modifications to the rules governing e-discovery in 2012.

Government's E-Discovery Obligations: Beyond Civil Litigation

While several courts have previously recognized that the government, as a civil litigant, is subject to the same e-discovery rules as any other civil litigant, the government's e-discovery obligations under FOIA came under scrutiny in 2011. Judge Shira Scheindlin of the District Court for the Southern District of New York found that the government was subject to the same or similar e-discovery obligations under FOIA as those set forth in the Federal Rules of Civil Procedure, including holding that metadata was part of the public record and, therefore, should be produced upon request under FOIA (subject to the applicable FOIA exemptions).[vii] As counsel to plaintiffs in this action, Mayer Brown played a critical role in the decision, helping to shed light on the deficiencies in the government's collection and production process and helping to pull back the curtain on misguided actions by the federal government. Although Judge Scheindlin subsequently withdrew her opinion, the case ignited a firestorm of debate over the government's e-discovery obligations under FOIA.

Social Media

Several 2011 court rulings have borne out the predictions we made last year with regard to social media in our "2010 Trends in E-Discovery." These decisions clearly demonstrate the unassailable truth that relevant information will be discoverable regardless of how that information is generated or where that information is stored. As a result, the courts have continued to allow litigants to discover relevant information posted to social media websites.[viii] And, as the use of social media continues to grow, so too does the wealth of information subject to discovery.

E-Discovery Costs

A great deal of attention was paid to e-discovery costs in 2011, with several decisions allowing prevailing parties to recover at least some of the costs of e-discovery.[ix] Pursuant to Federal Rule of Civil Procedure 54(d) and 28 U.S.C. §1920, the victor in a lawsuit may recover certain costs from the losing party. While there remains some dispute as to whether or which e-discovery costs are covered by 28 U.S.C. §1920,[x] it is clear that litigants should consider the potential of recovering costs in their e-discovery strategy and the potential recovery of such costs may be a powerful motivator in encouraging parties to cooperate in managing e-discovery costs.

For inquiries related to this summary of the 2011 Trends in E-Discovery, please contact any of the following lawyers.

Anthony J. Diana
adiana@mayerbrown.com

Michael E. Lackey
mlackey@mayerbrown.com

Therese Craparo
tcraparo@mayerbrown.com

Kim A. Leffert
kleffert@mayerbrown.com.

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

Ed Sautter
esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com

[i] *See, e.g.*, *Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency*, No. 10 Civ. 3488, 2011 WL 381625, at *8 (S.D.N.Y. Feb. 7, 2011) (stating that the expense of e-discovery could be diminished if parties were to cooperate and communicate regarding e-discovery issues), *withdrawn Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency*, No. 10 Civ. 3488 (SAS) (S.D.N.Y. June 17, 2011); *In re Facebook PPC Adver. Litig.*, No. C09-03043, 2011 WL 1324516, at *1-*2 (N.D. Cal. Apr. 6, 2011) (recognizing that e-discovery should be a "party-driven" process and the parties are "charged" with cooperating).

[ii] *See* http://www.nysd.uscourts.gov/events-exhibits.php (announcing launch of pilot program).

[iii] *See "An E-Discovery Model Order,"* http://memberconnections.com/olc/filelib/LVFC/cpages/9008/Library/Ediscovery%20Model%20Order.pdf.

[iv] Court of Chancery Guidelines for Preservation of Electronically Stored Information, January 2011.

[v] Act of June 23, 2011, Ch. S.L. 2011-0199 (N.C. 2011).

[vi] Supreme Court of Pennsylvania, Civil Procedural Rules Committee, Proposed Recommendation No. 249 (2011).

[vii] *See Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency*, No. 10 Civ. 3488, 2011 WL 381625, at *8 (S.D.N.Y. Feb. 7, 2011), *withdrawn Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency*, No. 10 Civ. 3488 (SAS) (S.D.N.Y. June 17, 2011).

[viii] *See, e.g.*, *Zimmerman v. Weis Mkts.*, No. CV-09-1535, 2011 WL 2065410 (Pa. Com. Pl. May 19, 2011) (holding that there is no reasonable expectation of privacy in social media and ordering production of passwords, user names and log-in names for MySpace and Facebook accounts).

[ix] *See Race Tires America, Inc. v. Hoosier Racing Tire Corp*, No. 2:07-cv-1294, 2011 WL 1748620 (W.D. Pa. May 6, 2011) (awarding prevailing party $367,400 in e-discovery costs); *Parrish v. Manatt, Phelps & Phillips, LLP*, No. C 10–03200 WHA, 2011 WL 1362112 (N.D. Cal. Apr. 11, 2011) (upholding award of costs of approximately $28,000 associated with counsel's reproduction, scanning and conversion of documents as "warming up the electronic discovery engine").

[x] *See, e.g.*, *Mann v. Heckler & Koch Defense, Inc.*, No. 08-cv-611, 2011 WL 1599580 (E.D. Va. Apr. 28, 2011).

Electronic Discovery & Records Management

Tip of the Month

Reducing the Costs of E-Discovery: Preservation and Proportionality

Scenario

An organization is named as a defendant in a large-scale antitrust class action filed in federal court. The organization's legal department immediately issues a broad preservation notice to personnel in nearly all of its domestic offices, suspends its email auto-delete function, issues preservation requests to its foreign affiliates and begins to consider extraordinary preservation efforts. One week later, the same organization is served with a complaint in a discrete employment matter involving the alleged wrongful termination of one of its sales associates. The organization, concerned about ensuring that it does not run afoul of its preservation obligations, contemplates whether its preservation plan for the employment action must be the same as that of the antitrust action.

The Organizational Costs of Preservation

The costs and burdens associated with the preservation and production of electronically stored information (ESI) can be significant. Commentators have remarked that many lawyers, as well as institutional, organizational, and governmental litigants, view preservation as one of the greatest contributors to the disproportionate costs of litigation in cases involving ESI. An organization issuing a widespread preservation notice may potentially face expenses associated with pulling backup tapes from rotation, imaging hard drives, searching for relevant data and suspending data retention policies, accompanied by the costs of processing, reviewing and producing large volumes of data.

But it is not simply the preservation or production of ESI relevant to one litigation that is cause for concern. Often overlooked are the long-term costs of cumulative preservation. Preservation of ESI in one matter can create a pool of discoverable data that must be considered for continued preservation and production in all subsequent legal actions. While this may, to some extent, be unavoidable, overbroad preservation efforts taken by organizations concerned about the uncertain legal landscape and the risk of sanctions compound the problem. For example, when an organization chooses to pull backup tapes from rotation as part of its preservation plan for one matter, those backup tapes must be replaced, stored, organized and managed, *and* they become a potential data source for every subsequent legal action.

Over time, the accumulation of data not otherwise needed for normal business operations, coupled with the regular influx of new legal matters (and new legal holds), makes disposing of *any* data increasingly difficult. Additionally, the costs associated with the increasing volume of preserved data—including managing and maintaining the systems that are required to properly house and organize the data, as

well as effectively search for, process, review and produce the data for each legal action—can be prohibitive.

Proportionality and Preservation

As some courts have observed, there is a distinct lack of consensus regarding the standards that should govern preservation and spoliation. That uncertainty has led many organizations to opt for expansive preservation efforts, regardless of the proportionality principles set forth in Rule 26(b) of the Federal Rules of Civil Procedure. Rule 26(b) identifies certain factors that may be considered in balancing the burdens of discovery against its likely benefits, including the risks presented by the legal action, the needs of the case, the amount in controversy, the organization's resources, the importance of the issues at stake, the importance of the potential discovery to resolving the issues, and whether the discovery sought is cumulative or duplicative or can be obtained from a more convenient, less burdensome or less expensive source. And while just about every litigant knows that relevant information must be preserved in the face of reasonably anticipated litigation, and that production may be limited by the concept of proportionality, less known is that some courts have recently shown explicit support for applying the concept of proportionality to preservation. These courts note that the concept of proportionality in preservation has been overlooked, or at least not articulated, in prior court decisions. In fact, at least one court has opined that a non-proportional approach seems out of step with Rule 26(b), which the court reads as cautioning that *all* permissible discovery must be measured against the yardstick of proportionality.

But beyond the recent case law, an organization should approach its preservation obligations with the same business and common sense approach applied to other legal decisions. What are the risks and issues at stake in the litigation? Who and what are the actual sources of responsive information? Do backup tapes really have information that is reasonably likely to be responsive *and* that is not available from another source? Is there a less expensive or burdensome way than imaging to preserve data on hard drives? A knee-jerk reaction that employs extraordinary preservation measures in every legal action may create more costs and burdens than benefits.

Best Practices: Develop a Flexible Preservation Plan

- *Understand the organizational costs of preservation and your options*. Know your company's data sources and the costs associated with preservation. Assessing the proper preservation method for a particular data source or legal action, and defending the method chosen, requires an understanding of how the organization's systems operate, what information is maintained by those systems, the options available for preservation or collection of data from each source and the costs associated with those options.
- *Consider developing a preservation policy which acknowledges that an appropriate preservation plan may depend on the circumstances of each legal matter.* All legal actions are not created equal. The preservation measures required are likely to vary depending on the scope of the claims, the legal and factual issues involved and the risks presented. A rigid preservation plan that demands a uniform response to all legal actions is likely to result in over or under preserving at some point. Consider working a degree of flexibility into your preservation policy so that you can appropriately address each legal action.
- *Think about negotiating preservation limits with opposing counsel*. Negotiating the scope of each party's preservation efforts, if possible, may help to avoid protracted and costly motion practice as discovery progresses. If an agreement cannot be reached between the parties, it may still be

useful to advise opposing counsel of the steps taken to preserve relevant data sources. This puts the burden on your adversary to object to your selected measures and explain why those measures are insufficient. Keep in mind that Rule 26(f) instructs parties to discuss any issues about preserving discoverable information during the meet and confer.

- *Consider developing policies and procedures that provide for the timely and effective lifting of legal holds.* Preservation obligations do not continue indefinitely, and a failure to timely lift legal holds may compound the costs and risks associated with preservation. Consider developing policies and procedures that allow for the timely and effective lifting of legal holds where possible and make sure those policies and procedures are enforced.

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

Cost- and Risk-Reducing Options for Production of Electronic Data

Scenario

A large financial firm is defending a class action law suit which includes fraud claims. The firm's investment process generates mountains of data, including not only email but also databases, spreadsheets, and proprietary file formats used by internal systems. Metadata will likely also constitute responsive data. The company's General Counsel is interested in minimizing the litigation costs, including the cost of production.

Measuring Production Costs

When deciding which production method would be most cost-efficient, it is important first to decide how costs should be measured. In cases with substantial data produced by both sides, it makes sense to consider not only the cost of producing one's own data, but also that of reviewing files produced by the opposing side. Conversely, if the bulk of the data is produced by one party, the cost of reviewing materials produced by the other side is not directly relevant. Even then, a production method that saves the other side money may be used as a bargaining chip during initial pre-trial conferences.

Note that the monetary cost of alternative discovery methods does not tell the whole story. Sometimes a method that costs more now can save money and reduce risk later. For instance, a more painstaking redaction process increases up-front costs but could prevent a damaging waiver of privilege. Parties should weigh known costs against resulting risk to determine which approach best suits their financial situation and risk tolerance in each litigation.

Producing Summaries or Compilations

With document review commonly accounting for the lion's share of discovery costs, many litigants overlook opportunities to save production costs by considering alternatives to the common approach of mailing DVDs of tagged image file format (TIFF) files. Creating a summary or compilation of voluminous data can be an effective way to save time and resources when producing data, particularly when a database is responsive to a discovery request.

Databases are huge files that can change frequently. Often a snapshot of the database is produced in full, but this method may sever links to other parts of the database, rendering its macros and other internal links unusable. This can cause disputes when the receiving party cannot fully use the data.

However, if only a small percentage of the data is relevant and responsive, the requesting party might accept targeted database *reports*, summarizing relevant slices of the database, in lieu of a database snapshot.

Similarly, relevant data might be spread across thousands of documents from which privileged or irrelevant data must be redacted prior to production. The producing party can consider generating a summary encapsulating all the relevant data from the underlying documents. This can save on both review and redaction costs.

Discussing options for data summaries or compilations is appropriate at initial pre-trial conferences pursuant to Federal Rule of Civil Procedure 26(f) or analogous state or regulatory rules.

Native Format vs. TIFF

Data is often produced in TIFF format, but it may be more efficient to skip the TIFF conversion and deliver files in their native format.

Native-format production eliminates the conversion step, which can be costly and complicated for large files such as spreadsheets, databases and computer aided design (CAD) drawings. When metadata is important, native-format production curtails the debate over the sufficiency of such production because all of the metadata is automatically included. This approach also retains complex relationships that are not easily represented in two-dimensional TIFF files, making spreadsheets and engineering drawings significantly easier to review and understand.

Alternatively, conversion to a non-modifiable, printable format, such as TIFF, brings several advantages. TIFF files are easy to redact, while redaction in native format is technically more complicated and could bring the risk of a spoliation claim. Further, with TIFF production, what you see is what you get, while native formats may contain hidden data that must be revealed and reviewed prior to production. Also, conversion to TIFF is predictable and repeatable, which can simplify foundational questions and allay fears of fabrication.

However, this need not be an all-or-nothing decision. Production could proceed in native format for some data, such as spreadsheets and drawings, and in TIFF for others, including emails and text documents. This takes into account the capabilities of the chosen document review tools, the amount of information lost in conversion to TIFF from each format, and the various formats' respective propensities to hide potentially privileged or confidential materials. Similarly, native format could be used for some custodians, while those custodians likely to possess privileged or private information can have their materials converted to TIFF, to enhance the ability to review and redact, prior to production.

Transfer Method

Finally, when the files have been gathered and redacted, how should counsel deliver them to the opposing side? Typically, a hard drive, CD or DVD is mailed or hand delivered to opposing counsel, but secure ftp sites offer an alternative that could reduce both cost and risk.

With traditional mailing or delivery, the disk could be lost or misdirected, resulting in delay and possible security breaches. Alternatively, materials uploaded to a secure site are encrypted with keys known

only to the two parties, reducing the risk of misdirection and increasing the speed of transfer. These "cloud" solutions facilitate rolling productions, as files can be uploaded as they are ready to be produced, without the need to wait for a sufficient amount of data to justify generating a new disk.

Conclusion

The final stage of discovery, in which materials are actually delivered to the opposing side, might seem like a routine occurrence offering few significant choices. However, considering the generation of compilations or summaries, evaluating TIFF and native-format production, and opting for non-physical delivery could all offer substantial savings in suitable circumstances. Litigants can benefit by actively considering such innovative solutions at the beginning of the discovery process and discussing them with opposing counsel well in advance of actual production.

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

Please visit us at www.mayerbrown.com

Electronic Discovery & Records Management

Tip of the Month

Balancing the Costs of Privilege Review with the Risks of Waiver

Scenario

A large financial institution is responding to discovery requests in connection with an investor suit relating to certain financial products marketed by the institution. To minimize the costs, the financial institution directs its outside counsel to use search terms to identify potentially privileged documents and to limit attorney review to only those documents that hit on the privilege search terms. Later in the litigation, the financial institution seeks to claw back more than 100 privileged documents that were inadvertently produced. Plaintiffs return the inadvertently produced documents, but move to compel their production and the production of all documents relating to the subject matter of those documents. Plaintiffs argue that given the financial institution's review methodology, the production of the privileged material was not inadvertent and effectively waived protection as to both the specific documents and the subject matter.

Federal Rules of Evidence 502

There is increasing pressure to use advanced technology to help curb the costs associated with electronic discovery. But in doing so, organizations and their counsel should be mindful of the significant risks posed by taking shortcuts when it comes to a privilege review. Rule 502 of the Federal Rules of Evidence was amended in 2008 to address concerns about increased costs of electronic discovery. In particular, the amendments address concerns about the burden involved with attempting to ensure that no privileged documents "slipped through the cracks" of voluminous document productions, and to make clear that the inadvertent production of privileged material does not constitute a broad subject matter waiver.

Rule 502 states that the disclosure of privileged material will not operate as a waiver in a federal or state proceeding if (i) the disclosure is inadvertent; (ii) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (iii) the holder promptly took reasonable steps to rectify the error. Generally, the key consideration in determining whether a waiver occurred is whether the steps taken by the producing party were "reasonable."

The Advisory Committee notes to Rule 502 indicate that relevant considerations include: "reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issue of fairness." The Advisory Committee also explicitly recognizes the potential use of technology: "a party that uses advanced analytical software applications

and linguistic tools in screening for privilege and work product may be found to have taken 'reasonable steps' to prevent inadvertent disclosure."

Some organizations have taken Rule 502 to mean that the use of technology to screen for privilege and work product will relieve the organization of the need to manually review those documents. But the courts do not necessarily agree.

Federal Court Scrutiny

Courts have expressed skepticism toward decisions to rely primarily upon technology to screen for privilege or work product. For example in *Mt. Hawley Ins. Co. v. Felman Production, Inc.*, a West Virginia magistrate judge found that the steps taken by the plaintiff to prevent an inadvertent disclosure were not sufficient, despite the facts that the plaintiff had, among other things: (i) hired an outside e-discovery vendor; (ii) identified, applied and tested search terms to locate privileged documents; (iii) identified, applied and tested searched terms for relevant, non-privileged documents; and (iv) conducted an attorney review of the relevant documents prior to production.[1]

Remarkably, in affirming the magistrate judge's order that a waiver had occurred, the district court noted that it did not have to review the process for screening for privileged material because "[t]he ridiculously high number of irrelevant materials and the large volume of privileged communications produced demonstrate a lack of reasonableness."[2] This decision may indicate that what is relevant in determining whether a procedure is "reasonable" is not only the privilege review itself, but also the procedures employed in the overall document review and production process.

Mt. Hawley Ins. Co. is not an aberration. For example, a Maryland court cautioned that "while it is universally acknowledged that keyword searches are useful tools for search and retrieval of ESI, all keyword searches are not created equal; and 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 for privilege review."[3] And yet another court, this one in Pennsylvania, noted that "[a]n understandable desire to minimize costs of litigation and to be frugal in spending a client's money cannot be an after-the-fact excuse for a failed screening of privileged documents…".[4] Technology, therefore, may not be the panacea for every organization's concerns about the rising costs of electronic discovery.

Best Practices for Leveraging Technology in Privilege Review

Organizations should not avoid the use of advanced technology for fear of waiver. Rather, organizations and their counsel should carefully consider the risks involved in relying primarily upon technology to help curb the costs of a privilege review, and they should take the time to develop a review workflow that balances the need to minimize costs with the risks of inadvertent waiver.

- Maintain an up-to-date list of attorney names (both inside and outside counsel) and law firms that may appear in privileged or work-product protected material. Providing accurate information to your outside counsel and review team will increase the likelihood of an accurate privilege review.
- Establish a set of search terms specifically designed to identify potentially privileged or work-product material based on terminology used within your organization. The more specific your

search terms, the more likely they are to capture potentially privileged documents and withstand scrutiny.

- Evaluate the available technology, including the risks associated with that technology, and conduct tests with samples of your organization's data to ensure effectiveness. Understanding how the technology works and implementing controls to address any risks may be effective in defending the reasonableness of your procedures.
- Assess which combination of technology and manual review will be most effective for the matter at hand given the costs, the type of data, and the risks at issue in the legal matter. Not all technology, data sources or legal matters are created equal.
- Consider consulting technology professionals or e-discovery counsel. Technology professionals and e-discovery counsel may be able to offer insight into creative approaches for tackling mountains of data.
- Enter into a clawback agreement in accordance with Federal Rule of Evidence 502(e) that includes an express provision detailing the procedure for requesting the return of potentially privileged material.
- Carefully manage and document the review process regardless of the technology selected. Educated and knowledgeable counsel are more likely to convince a court that the process selected was reasonable.

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

[1] *Mt. Hawley Ins. Co. v. Felman Production, Inc.,* No. 3:09-cv-00481, 2010 WL 1990555 (S.D. W.Va. May 18, 2010).

[2] *Felman Production, Inc. v. Industrial Risk Insurers*, No. 3:09-0481, 2010 WL 2944777 at *3 (S.D. W.Va. July 23, 2010).

[3] *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 256-57 (D. Md. 2008).

[4] *Rhoads Industries, Inc. v. Building Materials Corp. of America*, 254 F.R.D. 216, 227 (E.D. Pa. 2008).

Electronic Discovery & Records Management

Tip of the Month

Using E-discovery Tools to Reduce the Burden and Cost of Privilege Logs

Scenario

Two large companies are at the discovery stage of a breach of contract dispute pending in federal court. There was a great deal of negotiation leading up to the drafting of the contract by in house and outside counsel for both sides. As a result, a significant portion of the potentially responsive documents are protected under the attorney client privilege or the attorney work product doctrine. The general counsel of one of the litigants wants to know how to reduce the burden and cost of producing what is likely to be a massive privilege log.

Production of Privilege Logs

It is no secret that the cost of litigation is rising, nor is it a secret that electronic discovery is, in large part, the major culprit. The burden and cost associated with preserving, collecting, reviewing and producing Electronically Stored Information (ESI) can be daunting. Indeed, a survey conducted by the American College of Trial Lawyers revealed that over 87 percent of respondents "indicated that e-discovery increases the costs of litigation" and that over 75 percent "agreed that discovery costs, as a share of total litigation costs, have increased disproportionately due to the advent of e-discovery." One aspect of discovery, and e-discovery in particular, that contributes significantly to discovery costs is the privilege log. There are, however, ways that litigants can minimize the burden and costs that result from creating and defending privilege logs.

The Federal Rules of Civil Procedure require a party wishing to withhold information based on privilege to provide, in a privilege log, sufficient detail to enable the other party and the court to assess the applicability of the claim. Failure to provide sufficient detail has, in some cases, led courts to hold that the privilege is waived.

A typical privilege log, at a minimum, should include:

- The type of document being withheld;
- The date it was created or last modified;
- The document's creator (i.e., the "author");
- Where the document was found (i.e., the custodian);
- The documents' subject or title;

- To whom the document was sent to (e.g., to, cc and bcc); and
- A description and justification of the privilege being asserted.

When you consider that it is not unusual, in information-intensive cases, to have hundreds, if not thousands, of emails and other communications to assert privilege over, reviewing and manually entering each of these fields in to a log can be tedious, time-consuming and expensive. And while Federal Rule of Evidence 502 was enacted in 2008, in part, to address the fact that litigants were incurring these costs to simply protect against the inadvertent waiver of attorney-client and work product privileges, courts are generally not receptive to arguments that the burden of a privilege review should justify limiting discovery.

Reducing the Burden and Cost of Privilege Logs

There are other ways, however, that parties can minimize the burdens and costs associated with conducting a privilege review and preparing a privilege log when large volumes of data are involved. These options include the creative use of the meet and confer process and the creative use of technology. For instance, parties should consider using the meet and confer process to:

- Limit the types of communications that must be included on a privilege log—e.g., agreeing that communications with outside counsel need not be logged or that privileged communications after the filing of the complaint need not be logged;
- Limit the universe of documents subject to full logging to a restricted set of custodians and producing only basic information—i.e., the type of information that can be electronically generated from most electronic document review tools today—for all other privileged documents;
- Agree to logging email chains as one document;
- Agree to logging only one instance of each document, with the understanding that exact duplicates do not need to be logged;
- Agree to withhold partially privileged emails in their entirety rather than incurring the costs of redacting the privileged portions; and
- Agree to describe general categories of privileged documents, (for example, time period, names of individuals on communications, or general description of type of content of communications), with sufficient information for the parties to determine whether a more detailed log would be necessary for categories that may be in dispute.

The creative use of technology can also help to reduce the cost and burden of privilege review and privilege log preparation. Most e-discovery vendors have robust search and email thread logic tools that allow parties to quickly find relevant documents. The same tools can be applied to search for potentially privileged materials, including the names of attorneys and the domain names of law firms, or emails with the words "attorney client" or "privileged" in the subject line. In addition, some e-discovery tools can identify "near duplicates" or use concept searching to identify potentially privileged documents that may not be captured using search terms.

Once these documents are collected, many e-discovery tools can electronically create a draft privilege log. By using the document's metadata, the e-discovery tool can export basic information about a potentially privileged document to an Excel spreadsheet, including the document's sender, recipient,

subject, etc. If the reviewers also code certain fields during the review, either indicating the type of privilege, or putting in descriptions or attorney names, that can also be exported to an Excel spreadsheet. This can help to limit the amount of review for any given document in that the document may only need to be reviewed once in order to determine privilege and prepare the privilege log. While any electronically created privilege log must be reviewed and revised to meet the needs of a particular case or rules of a specific jurisdiction, having the privilege log created automatically saves a huge amount of time and resources over the manual process of adding one document at a time to a spreadsheet.

While these options may not entirely eliminate the cost of creating a privilege log for any given case, they can certainly decrease cost and increase efficiency.

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 Ethan Hastert at ehastert@mayerbrown.com.

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

Please visit us at www.mayerbrown.com.

May 2011

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Costs of E-Discovery: Post-Production

Scenario

An organization is involved in a litigation involving significant volumes of electronic data. After enduring the costs of processing the data, the organization finds itself faced with the additional costs of managing and maintaining not only its own production data, but also the data produced by other litigants. As the production volume mounts, the organization becomes increasingly concerned with the growing costs of managing the post-production data over the life of the matter. The organization begins to explore potential options for managing the costs of post-production data as it continues to evaluate the productions and prepare for trial.

Best Practices for Managing the Costs of Post-Production E-Discovery

There is a great deal of focus on managing e-discovery costs pre-production, but far less discussion about how to manage these costs post-production. Yet post-production costs can be significant and can extend over long periods of time. Litigants and their counsel should think creatively about how to manage those costs, including leveraging the same types of technologies that are used pre-production, limiting or eliminating certain costs as soon as possible and leveraging work product across litigations.

Consider Corporate Cost Savings Initiatives

- *Preservation Planning.* In addition to establishing a process for *implementing* legal holds, organizations should establish a defensible process for *lifting* them. Establishing such a process allows an organization to minimize the costs of ongoing preservation and to return to its "business-as-usual" records-retention policies as soon as possible. Ensuring that legal holds are *actually* lifted is just as important as establishing the defensible process in the first place; policies and procedures are effective only when they are put into use by the organization.
- *Data Collections Tracking Database:* Organizations facing frequent, or repeat, litigation should consider developing a database to comprehensively track the history of each data set collected for a legal matter, including details about date ranges, custodians, data sources and restrictors (as in the case of keyword-driven collection). By maintaining this database, an organization will be able to track how the datasets were processed, if the documents are available in native

and/or TIFF formats and, most importantly, where the data resides (e.g., in-house, outside counsel or e-discovery provider). This resource will help determine whether the data can be archived offline at lower cost, deleted, or repurposed for a new matter (thus avoiding repeat collection cost).

Negotiate with Your Third-Party Provider

- *Ensure Vendor Contracts Include Post-Production Cost Saving Measures.* Negotiate upfront with your provider for lower hosting charges based on the phase of the litigation. For example, press for a reduction in storage charges when review and production has been completed and fewer users are accessing the database, and negotiate a reasonable export charge with an eye toward moving the production data to a lower-cost hosting provider or bringing the data in-house if you have an appropriate database environment. Maintain unnumbered TIFF images for repurposing, and contract with your provider to reuse (by re-endorsing) these images when applicable to other matters. Establish reasonable fees for your provider to dispose of (or return) your data and close out any hosting engagement.
- *Practice Thrifty Data Management**.*** Even the most basic data management efforts can save an organization thousands of dollars. For example, make sure to direct your provider to archive raw collection data to inexpensive backup media once that data has been superseded by its production form, and end hosting engagements as soon as possible to alleviate ongoing costs. Look for opportunities to reuse hard-drives or other storage media when it is no longer necessary to maintain the existing data on that media.

Utilize Proactive Discovery Strategies

- *Negotiate Production Formats.* Organizations should keep post-production efficiencies in mind during pre-production negotiations. For example, the most common production formats remains TIFF images accompanied by metadata and text load files. While these formats allow for full-text searching, and even some advanced near-duplicate document detection that can enhance post-production analysis, they can preclude the use of most early case assessment (ECA) tools, which generally rely on native files to deliver full benefit (e.g., ECA features that enable visual analysis of relationships between witnesses greatly enhance deposition preparation while providing more efficiencies over the traditional method of reviewing documents that hit on witness names). TIFF images also increase post-production costs because of the large size of the files. In some instances, it may be useful to consider opportunities to request native format production for file types (such as email) that benefit from ECA tools or file types that consume less space natively than in TIFF form.
- *Utilize Advanced Technologies.* A review of every page of every document produced by an opposing party is a near impossibility in large, document-intensive litigation. ECA, near-duplicate technologies, concept searching and other tools designed to organize and categorize documents can be used not only for pre-production review, but also for post-production analysis. These tools enable an organization to identify hot documents, prepare witness kits and trial exhibits, or identify deficiencies in an opponent's production in a timely and cost-effective manner.
- *Sharing E-Discovery Provider Services.* Consider sharing a single e-discovery provider to host the post-production data from all parties, including opposing parties. By controlling end-user

access rights, confidentiality for all parties is maintained, while significantly reducing costs.

- *Leveraging Work Product.* Reusing data from other litigations can minimize future e-discovery costs. Where appropriate, organizations can work with their providers to extract the relevant data for use in any new matters. Consider also taking advantage of existing search term lists and privilege logs to reduce cost *and* time.

Post-production costs can add up over time, but by being proactive it is possible for organizations to manage these costs. Making the effort to inject post-production considerations into your earliest discussions (and planning) – both internally and with your adversaries and providers – can result in quantifiable cost savings.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, Therese Craparo at tcraparo@mayerbrown.com, Allisa L.V. Vermillion at alvvermillion@mayerbrown.com, or Patrick Garbe at pgarbe@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

June 2011

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

E-Discovery and Data Privacy in the US

Scenario

An online retailer collects personally identifiable and private information about its customers, including their names, addresses, email addresses, cell phone numbers, birthdates, credit card information and "rewards points" account numbers for hotels and airlines. The retailer recently received a document request for "all information collected about each of your customers." The retailer's General Counsel is concerned not only about whether some or all of the information will be required to be produced, but also about how to protect the privacy rights of its customers in the event that production of the personal information is ordered.

Data Privacy and Discovery

Data privacy is one of the most hotly debated topics in both legal and business circles in the United States. Increasing cyber-attacks and high-profile data breaches have brought attention to the risks associated with a failure to protect the personally identifiable information of an organization's customers and employees. While references to data privacy and data protection often bring to mind the highly developed data protection laws in the European Union, there are numerous data privacy laws in the United States that affect the way organizations do business, including:

- Gramm-Leach-Bliley Act (GLBA)
- Right to Financial Privacy Act (RFPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic & Clinical Health (HITECH) Act
- Children's Online Protection Act (COPA)
- Payment Card Industry Data Security Standards (PCI DSS)
- State Breach Notification Laws
- State Data Transfer Laws

However, while many organizations employ privacy professionals, and are aware of their data privacy obligations in their day-to-day business operations, personally identifiable information that is collected in response to a document request often falls into the "black hole" of litigation. That is, once that data

is collected for litigation, the organization stops scrutinizing whether the steps being taken to protect against data breaches or unnecessary disclosure are sufficient to meet the organization's legal obligations and minimize the risk of data breaches. While many organizations have policies and procedures protecting the private data of employees and customers in their every day business activities, those same organizations often overlook the importance of applying those polices and procedures to e-discovery.

Given the emphasis on disclosure in US litigation and the frequent lack of coordination between data privacy professionals and in-house and outside counsel, the management of personally identifiable information in litigation represents a key area of risk. It is important for organizations and their counsel to recognize that there *are* risks associated with inadvertent disclosure and/or data breaches in the course of discovery. For example:

- In-house counsel will often apply the same over-collection philosophy to both non-private and private data.
- Data may be transferred to outside counsel or e-discovery vendors without proper data security measures.
- Organizations frequently fail to scrutinize their e-discovery vendors to ensure that those vendors are providing the same security protections that the organization itself is required to apply.
- Organizations often enter into (or permit their outside counsel to enter into) contracts with e-discovery vendors that do not contain sufficient protections against potential data breaches.
- Outside counsel may not apply the same level of scrutiny to protect personally identifiable information as is applied to privileged or other protected data.

There are ways to manage and mitigate the risks of data breaches associated with litigation. Considering data privacy issues at the outset of the discovery process can help limit the burdens and also minimize risks of producing private data.

Reducing Risks Through the Information Life Cycle

In-house and outside counsel should consider how to limit the transfer of private data and reduce the risk of a security breach at each stage of the information life cycle in the discovery process, e.g., collection, processing and production. For example, can the collection of personally identifiable information be limited at the outset of the litigation? Can the dissemination of that information be limited through confidentiality agreements and limits on third-party disclosure? If private data will be stored until the matter is finally resolved, what steps are necessary to ensure that the data is maintained securely? And, what procedures are necessary to ensure that any personally identifiable information is securely transferred?

Best Practices

- *Understand where protected information resides.* It is important to assess what personal data your business collects and uses, what privacy laws apply to that data and what your current practices may be with respect to the use and sharing of that data. To accomplish all this, many businesses employ privacy professionals or otherwise appoint a privacy team comprised of

individuals from human resources, legal, marketing, communications, technology, finance, strategy and other departments. When litigation commences, litigators can confer with such privacy staff to understand what types of information are collected in the course of business that are subject to privacy protection.

- *Leverage existing resources.* A business' privacy group typically has controls in place to manage private data. Litigators can consider applying these existing procedures to manage such data in the course of discovery.
- *Negotiate what should be collected and produced.* Negotiating the scope of data to be collected and produced with opposing counsel at the outset can help to reduce the amount of unnecessary and non-responsive data collected. It may also help to have candid discussions with opposing counsel regarding the scope of their requests. The requesting party may not realize they are asking for highly confidential information, and they may not want to be in possession of such information and expose themselves to the risks of a data breach. For example, the requesting party may want customer names and addresses, but not need customer birthdates or credit card information.
- *Organize data.* It is helpful to organize collected data so that segments containing private information can be targeted by the document review team and treated more efficiently.
- *Protect private data that must be produced in discovery*. The litigation may require that confidential and private information be produced. In such cases, it is common for the parties to enter into confidentiality agreements that dictate how this 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 (e.g., for attorneys eyes only).
- *Ensure vendors are protecting private data.* Private data can be most vulnerable to security breach when it leaves the business. Thus, when e-discovery vendors are used to process data in litigation, consider security safeguards including transferring only encrypted data, ensuring that the vendor has sufficient security and privacy protocols, and limiting access to the data by the vendor's staff.

Protecting private data is the responsibility of both in-house and outside counsel. Knowing where private data is kept, leveraging your business' existing resources for managing such data, negotiating the scope of production and having policies and procedures to protect that data will limit the risks of inadvertent loss when production is required.

For inquiries related to this Tip of the Month, please contact Kim A. Leffert at kleffert@mayerbrown.com, Seema V. Dargar at sdargar@mayerbrown.com, or Michael Lackey at mlackey@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, Jr. at mlackey@mayerbrown.com or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com

Electronic Discovery & Records Management

Tip of the Month

Managing International Data Privacy Concerns in E-Discovery

Scenario

An international organization with offices in both the United States and France is sued in the United States for fraud. Much of the data relevant to the US litigation is located on centralized servers in France, although the data can be accessed by individuals in the United States. The organization is unsure whether or how it can produce that data in the US litigation without running afoul of France's data privacy laws and blocking statute.

Data Consolidation & Globalization

Given the impact of globalization and cross-border ownership, it is not uncommon for information sought in discovery in US proceedings—including electronically stored information (ESI)—to be located outside of the United States. Access to such information is complicated by the unique and often differing perspectives of various foreign jurisdictions toward the discovery or disclosure of such information.

In addition, many organizations are moving, or have already moved, toward "cloud computing" models, which consolidate the organization's and its affiliates' information technology infrastructure and services in order to improve consistency in data management, manage costs and improve efficiency. Those cloud computing models have the potential to further complicate the legal questions that arise in connection with US discovery.

International Data Privacy & E-Discovery

While the United States has a discovery system that encourages extensive production of information, many other countries have far more protective schemes. In particular, the European Union Member States have detailed data protection laws based on the European Union's Data Privacy Directive. Those laws tightly regulate when and how personally identifiable information (which encompasses a broad range of information including name, age, gender, marital status, nationality, citizenship, veteran status, personal or business contact information, identification numbers, etc.) may be collected,

processed, stored and transferred by an organization.

In addition, several European countries have enacted blocking statues designed to protect sovereignty and shield foreign nationals from intrusive US-style litigation. Violations of these foreign laws may result in serious consequences for the organization, including criminal charges. Taken together, these laws create a tension between the mandate of the US Federal Rules to produce all relevant electronic records and the laws regulating discovery and transmission of ESI abroad.

There are several questions an organization will face when determining whether data located abroad must be produced in a US litigation. First, what are the conditions under which ESI stored outside of the United States is deemed to be in a domestic party's "possession, custody, or control" under the Federal Rules of Civil Procedure? Consistent with the emphasis on full disclosure in the American legal system, US courts construe the term "control" broadly. Thus, a party often will be deemed to have control if it has the legal right, authority or practical ability to obtain the materials sought upon demand. Second, does the applicable foreign law permit the processing, transfer and production of overseas ESI? The answer to this question will depend on location of the data and the laws of the country at issue. Third, will the US courts require the production of relevant data regardless of any foreign restrictions? The answer to this question is generally "yes," although US courts have proved more willing to give deference to restrictions arising from data privacy laws than those arising from foreign blocking statues.

Best Practices for Managing International Data Privacy Issues in E-Discovery

Because the US courts tend to require the production of relevant data in an organization's possession, custody and control regardless of any foreign restrictions, it is helpful for an organization to consider the best ways to ensure that it can meet both its US and foreign legal obligations. As with any effort to manage and minimize risks, the best practice is to evaluate those risks before litigation arises and implement standard controls.

- *Know Your Data & Your Legal Obligations*. Every organization should be familiar with the laws governing its data and how that data may be collected, processed, retained or transferred *before* litigation commences. Involving local counsel and data privacy professionals in the litigation process will help to minimize the risks associated with the collection, processing and transfer of data in connection with US litigation and ensure that the organization does not violate its local rules and regulations.
- *Limit Collection*. A good way to help to minimize the risks associated with collecting, processing and transferring data located abroad in connection with a US litigation is to limit the scope of the data at issue in the litigation. Litigation counsel should negotiate the scope of data to be produced with opposing counsel in an effort to reduce the amount of unnecessary and non-responsive data collected. And an organization should consider implementing collection procedures that are specifically targeted at identifying relevant data from the outset, rather than employing a broad collection philosophy and relying on the review process to narrow the data for production.

- *Consider On-Site, In-Country Review*. In some instances, an organization may facilitate its ability to collect and process data relevant to a US litigation by conducting the review of that data in the country where the data is located. This review will help to identify only the information that is actually relevant to the US litigation before it is transferred, and may minimize the quantity of personally identifiable information at issue.
- *Consider Redaction or Anonymization*. Even where data located abroad is relevant and must be produced in a US litigation, it may not be necessary to produce data that constitutes personally identifiable information. Use of anonymization techniques or redaction of personally identifiable information may address an organization's data privacy obligations.
- *Evaluate Transfer Options*. An organization may retain responsibility for ensuring that personally identifiable information is protected in accordance with the laws of its place of origin, even after the data is transferred to the United States. There are various options for such transfers, (e.g., use of "Safe Harbor" vendors, employing the Hague Evidence Convention procedures, negotiating vendor contracts that include model contractual language or other provisions designed to ensure the data protection, or implementing strict protective orders); however, depending on the circumstances, use of these methods of transfer will not necessarily satisfy data protection requirements.

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

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

Please visit us at www.mayerbrown.com

Electronic Discovery & Records Management

Tip of the Month

Preserving Electronically Stored Information When Employees Depart

Scenario

A large company announces a reduction in force of several thousand employees. The company's head of litigation knows that at least some of those soon-to-be-terminated employees are subject to a litigation hold and wants to ensure that data is not lost or misplaced as a result of employees leaving the company.

Planning for Employee Departures

Regardless of the reason for an employee's departure, it is likely that an employee in career transition is not thinking about the employer's legal obligation to preserve electronically stored information (ESI). Likewise, the IT department is focused on managing assets (e.g., PC's, laptops, PDA's) and server space (e.g., email servers, personal drives on network), and views an employee departure as an opportunity to reduce IT-related costs. Nevertheless, a company's obligation to preserve ESI relating to current or anticipated litigation remains in place regardless of any workforce reduction.

Courts and regulators have increasingly focused on the risk of destruction of data of departing employees who were subject to a legal hold, and they both require that companies make good faith, reasonable efforts to preserve ESI of departing employees that is subject to a legal hold. Therefore, it is important for a company to implement procedures aimed at preserving, and collecting if necessary, ESI associated with its departing employees.

The Employee Left, but Not the Laptop

While it is common for companies to reuse electronic equipment after an employee leaves the organization, doing so can result in the inadvertent destruction of ESI subject to a legal hold. IT departments managing a company's computers, storage devices and "smart phones" or similar devices often do not learn that information stored on a departing employee's device may be subject to a legal hold until after the equipment has been wiped clean and reissued.

One way to preserve ESI while promoting the reuse of company equipment is to institute a waiting period before reintroducing previously used electronic devices back into the current workforce. The exact length of any waiting period depends on the size and culture of the company, but it should be long enough to allow for the company to determine whether any departed employees were subject to

an existing legal hold. The waiting period should also provide sufficient time to coordinate any data preservation measures if needed.

During this waiting period, a company should not delete any of the departing employee's emails or other ESI. Ensuring your company has enough time to determine whether it should preserve a former employee's electronic data before reusing the electronic equipment (or deleting the data) is an excellent way to help avoid the inadvertent destruction of ESI.

If possible, the company should develop standard operating procedures around the management of ESI of departing employees, so that the business, IT, records management, compliance and legal department each has a clearly defined role in making sure that ESI that should be retained, is retained, and, equally as important, that any ESI that need not be retained is destroyed in a timely manner consistent with the organization's document retention policies.

Alert New Employees that a Litigation Hold Is In Place

Another risk is when a new or reassigned employee enters into a situation unaware that a legal hold is in place. Therefore, it is important to promptly identify those new employees who inherit data subject to a legal hold. That new, or reassigned, employee should be informed of the company's obligation to preserve the data in the former employee's files and, if applicable, any continuing obligation to preserve future information moving forward.

Keep Litigation Hold Lists as Current as Possible

A company's personnel will not likely remain static for the duration of a lawsuit or investigation. Thus, companies should periodically review their litigation hold lists to determine whether any departed employees remain among the listed document custodians and, if so, whether any new employees who took possession of the departed employee's data should be added to the list. Companies that do not maintain lists of employees subject to a legal hold should consider implementing a process to retain this information in a convenient and accessible manner.

Investigate ESI Issues through Exit Interviews

Regardless of whether a company maintains a list of all employees who may be subject to a legal hold, it is prudent to institute a practice where all departing employees are asked prior to leaving whether their data is subject to a legal hold. Not only does this provide an opportunity to confirm where the data resides, but it also prompts the company to be alert to preserving a departing employees' information while transitioning employees out of the company. If the departing employees' responses are documented, this helps to create a record of the company's good faith efforts at preserving ESI.

In certain circumstances, a legal hold may extend to information stored on an employee's personal email, home computer, or other personal peripheral devices. For this reason, companies should also ask whether the departing employee ever used personal email or personal storage devices (such as thumb-drives) to store company ESI that is subject to a legal hold. With this knowledge, companies are better equipped to determine whether additional steps may be needed to preserve such data to ensure compliance with an existing legal hold.

Collecting ESI in Advance of the Downsizing

Corporate downsizing can put any company in a temporary state of flux. However, a company's ongoing duty to comply with legal holds remains unaffected. Consider taking proactive steps during this period to ensure that ESI is not accidentally lost along the way. These steps could include:

- Backing up the electronic data of employees subject to a legal hold in advance of any downsizing event;
- Collecting responsive ESI from departing employees; and
- Promptly revoking any former employee's ability to access company email or electronic devices immediately upon termination in order to prevent the accidental (or intentional) deletion of ESI by employees whose interests may no longer be aligned with the company's.

Dealing proactively with departing employees' ESI is good records governance regardless of any legal holds; however, the stakes are raised considerably when the ESI is subject to such a hold. When ESI subject to a legal hold goes missing, courts can respond by issuing sanctions and regulators can respond by refocusing their investigation on the company's compliance with subpoenas. Departing employees can compromise a company's ability to comply with its obligation to preserve responsive data. Therefore, companies should consider taking steps to ensure that changes in the makeup of its workforce do not impact the company's ability to satisfy its obligation to preserve ESI.

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 Bornhorst at mbornhorst@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

Electronic Discovery & Records Management

Tip of the Month

E-Discovery in Criminal Investigations

Scenario

A senior corporate executive is under investigation by the Department of Justice for accounting fraud. In the course of discovery, he learns that the investigators and prosecutors secured a warrant to seize a large number of personal emails from an Internet-based electronic mail service. The executive is unsure whether or not the prosecutors can lawfully make use of this material in their investigation or at trial.

Civil Litigation v. Criminal Investigations

Unlike their civil counterpart (and to the criticism of some), the Federal Rules of Criminal Procedure are largely silent on e-discovery. Thus, the rules governing e-discovery, while well-developed in the civil context, are far less developed in the context of a criminal investigation. Further, the nature of a criminal investigation materially impacts the rights of the parties involved to obtain and use electronically stored information. Targets of a criminal investigation—be they corporations or individuals—must walk a fine line between obstructing government investigators and vigorously protecting their rights.

When the government opens a criminal investigation, it has at its disposal a number of prosecutorial powers permitting the expansive collection of information about the target of an investigation. This includes issuing a grand jury subpoena directed toward documents and obtaining a search warrant directed toward the collection of data. However, the criminal nature of an investigation also affords the target certain protections that are not available in civil litigation. That is, the target of a criminal investigation may invoke the Fourth Amendment to shield the collection or use of certain data or the Fifth Amendment to protect against the potential testimonial nature of a document production.

Balancing the Rights of the Target with the Need to Investigate Suspected Illegal Activity

Given the dominance of electronically stored information in modern society and the prevalent use of electronic means of communication, it is not surprising that the government is frequently interested in gaining access to the electronic data of the target of an investigation. The question for the target thus

becomes whether he or she is afforded constitutional protections under the Fourth or Fifth Amendments that may prohibit or restrict the government's ability to obtain and use that electronic data. While the federal courts have previously considered (at least in the paper context) whether the act of producing a document itself may be sufficiently incriminating to invoke the Fifth Amendment, surprisingly, they are just beginning to grapple with the key question of how to balance the individual's expectation of privacy with the government's need to investigate suspected illegal activity when it comes to electronic data.

First, individuals do have a reasonable expectation of privacy in the content of certain electronic communications. Recent federal court decisions have made clear that, at least with respect to email communications, individuals have a reasonable expectation of privacy, and that the government is required to obtain a warrant in order to access and use that information in a criminal investigation and trial.

Second, even with a warrant in place, the government is not free to rummage through one's person or things. The Fourth Amendment requires that a warrant describe with particularity the place to be searched and the person or thing to be seized. Government agents conducting a warrant search must adhere to these restrictions. This can be a challenge with electronic data, as computers typically contain a great deal of information that is outside the scope of the criminal investigation. The government's potential need to examine large quantities of electronic records to investigate potential illegal activity thus raises difficult Fourth Amendment issues that are not present in a search of paper files.

Third, in yet another twist, the collection of large quantities of electronic records makes it more likely that those electronic files will contain attorney-client communications. Warrants increasingly require the government to take affirmative steps to avoid reviewing privileged materials, going so far as to require use of a "filter agent"—a disinterested investigator responsible for ensuring that case-investigators do not view privileged communications.

Fourth, the Supreme Court has recognized that the act of producing documents may be testimonial in nature: that is, by producing documents, a witness may be admitting that the documents existed, were in his or her possession or control, and were authentic. Accordingly, under some circumstances, the target of an investigation may invoke the Fifth Amendment to refuse to produce documents where the act of production itself may be incriminating. It should be noted, however, that there is a circuit split as to the availability of the "act of production" doctrine as applied to corporate representatives (although even where an individual produces records in his or her capacity as a corporate representative, the government may not introduce evidence that the documents were provided by a specific custodian).

Best Practices for Challenging the Seizure of Electronic Data

In challenging a search of personal electronic data, it is essential to consider the wide array of protections afforded by the Fourth Amendment and to ask the right questions.

Did the target have a reasonable expectation of privacy in the data obtained? The target should carefully consider the type of data obtained by the government, and whether the target had a reasonable expectation of privacy in that data (whether email communications or other types of data,

and even if the data is stored by a third party).

Did the government obtain a warrant? The government must obtain a warrant in order to properly obtain and use electronic data in which an individual has a reasonable expectation of privacy.

Did the warrant clearly state what was sought by the government agents in obtaining personal email? The government must specify what it seeks to obtain and must support its efforts with a showing of probable cause.

Did the warrant adequately limit the breadth of enforcement to those items for which the government had probable cause to search? Even where a warrant states with particularity the information sought, it must take additional steps to limit collection only to materials for which it has probable cause to examine.

Is it possible that the target's personal electronic data contained a request for, or receipt of, legal advice? If so, the government must take adequate precautions to ensure protection of these privileged materials. The government must adhere to any limitations on its search designed to protect the attorney-client privilege. Frequently, a filter agent will be employed to ensure that document materials are screened for confidentiality and privilege prior to review by the government. The filter agent must be unassociated with the prosecution.

Did the warrant contain material misrepresentations or omissions? If so, the target of a government investigation may be entitled to a Franks Hearing, where a court scrutinizes the government's efforts to secure a warrant.

Will the act of producing documents itself be incriminating? If so, the target of a government investigation may be entitled, under some circumstances, to refuse to produce the documents.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, Therese Craparo at tcraparo@mayerbrown.com, Patrick M. Kellermann at pkellermann@mayerbrown.com, or Michelle N. Webster at mwebster@mayerbrown.com.

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

Please visit us at www.mayerbrown.com.

October 2011

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Preparing for E-Discovery in Outsourcing Contracts

Scenario

A large US company recently outsourced its IT functions and has begun to use cloud computing vendors, or other service providers, to store or process data. The company's general counsel is concerned about any additional risks the company may face when responding to e-discovery requests, such as discovery penalties for inadequate preservation or incomplete disclosure, waiver of legal privileges and improper disclosure of confidential information to third parties. The general counsel is seeking ways to mitigate these risks through contract terms and advance planning.

Preserve Your Privileges

As a general matter, if your service provider has access to data that may fall within the attorney-client or work-product privileges, consider adding specific clauses to the provider agreement to protect any electronically stored information (ESI) that you have identified as potentially privileged. For example, the contract could provide for additional restrictions on disclosure, data tagging or segregation of potentially privileged information.

If you cannot specifically identify the privileged information, consider using a broad brush—e.g., requiring that the provider treat all communications to or from your corporate law department as potentially privileged. Or, if you are not aware of any particular privileged information, consider obtaining an option in your contract to designate information as protected at a later time; you may even agree to accept additional charges for such later-requested additional security.

Create a Litigation Response Plan

If your service provider will store ESI that may be subject to preservation or production requests, consider contractually requiring the provider to engage in developing and implementing a joint litigation response plan. Such a plan might involve, for example:

- A list of responsibilities for preserving the ESI described in any preservation or production request that can be identified with reasonable certainty, and for providing prompt notification of

any technical or other limitations that would prevent fulfillment of the preservation or production request;
- Participation in periodic meetings to discuss and update litigation response policies and procedures; and
- Appointment of an experienced legal information management representative by the service provider to manage production and preservation activities.

Provide Your Service Provider with a Litigation Requirements Notice

When litigation that has been filed, or is reasonably anticipated, relates to ESI possessed by your service provider, consider sending your provider a copy of the litigation hold notice that describes in reasonable detail all items to be preserved. Ask your provider to promptly contact you with any questions or concerns related to the notice and to provide you with any additional information you or the provider may need to more clearly determine the scope of the request.

Generate Information for Legal Proceedings

As litigation progresses, there are additional activities that you might want your service provider to undertake. For instance, you may request that your provider assist with the following:

- Cost estimates for the preservation and/or production of data;
- Descriptions of systems, data, media and processes utilized by the provider;
- Reports, declarations and affidavits from provider personnel; and
- Explained reasons why preservation or production of certain documents is infeasible or impossible in certain circumstances.

Regardless of the responsibilities assigned to your service provider—whether related to preservation and production or trial proceedings—it is recommended that you request that your service provider document, in writing, all steps taken to fulfill its obligations. This documentation helps ensure that your company's requests are being carried out in full, and provides evidence of your company's diligent efforts to comply with preservation obligations and discovery requests should your efforts come under scrutiny.

Third Party Data Requests

Opposing parties may request or demand access to your ESI from one of your service providers directly. There is a risk that a provider might provide ESI that should not be delivered to the opposing party. You can reduce that risk by including in your agreement or litigation response plan requirements that the provider:

- Immediately contact a company representative upon receipt of any request or subpoena by third parties for corporate ESI possessed by the provider and forward a copy of the request or subpoena to the company, to the extent legally permissible;
- Meet and confer with the company prior to responding to the third party(ies);
- Tender responsibility for responding to the request to the company and assist with any

responses; and
- Take all commercially reasonable steps to preserve the company's legal rights in connection with any response in the event the provider is barred from notifying the company of the request.

Recommendation

Having contractual obligations in service contracts and/or a litigation response plan can allow your company to handle discovery requirements faster, more effectively and with lower risk and expense when some or all of your data is managed by outsourced providers or cloud computing providers. Companies that do not already have these contractual provisions can attempt to amend their agreements with third-party providers that possess critical ESI. Consider including litigation readiness provisions as a standard requirement for new contracts and new relationships with outsourcing and cloud computing providers.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com, Brad L. Peterson at bpeterson@mayerbrown.com, or Shawna Doran at sdoran@mayerbrown.com.

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

Learn more about Mayer Brown's Business & Technology Sourcing practice or contact Brad L. Peterson at bpeterson@mayerbrown.com.

Please visit us at www.mayerbrown.com.

November 2011

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks and Costs of E-Discovery in Regulatory Investigations

Scenario

A financial institution is being investigated by the Securities and Exchange Commission (SEC) in connection with the institution's role as trustee in certain residential mortgage-backed securitization (RMBS) transactions. The financial institution receives several subpoenas from the SEC seeking detailed information about every RMBS transaction in which the financial institution was involved. The financial institution is concerned about the burden of responding to the SEC subpoenas, but is also concerned about appearing uncooperative and inviting even more scrutiny from the SEC.

E-Discovery Complications in Regulatory Investigations

Organizations face serious consequences for the failure (or the apparent failure) to cooperate with regulatory investigations. The general challenges related to the preservation, collection and production of electronically stored information (ESI) are compounded by several factors, including: (i) the risks related to regulatory investigations, (ii) the frequency of such requests, (iii) the possibility that different regulators and government agencies will share information among themselves about an organization's compliance with subpoenas or requests for production, and (iv) the reality that the regulator requesting the documents will not have a reciprocal obligation to produce documents, and thus it has less of an incentive to negotiate a solution that would reduce the burden and cost of the production.

In practice, if not in form, neither the Federal Rules of Civil Procedure nor their state rule counterparts govern most requests from regulators, and an organization's ability to seek relief from unduly burdensome requests, is limited by its fear of appearing uncooperative during a regulatory investigation. It is with these challenges in mind that an organization must prepare for, and comply with, requests for production in connection with regulatory investigations.

When conducting an investigation, regulators are often focused on recurrent issues that have arisen in many of their prior investigations. An organization should be aware of, and prepared to address issues such as:

- Inadequate systems or procedures exist to ensure the retention of information that needs to be preserved
- Difficulties in timely retrieval and production of relevant data

- Insufficient coordination between legal and IT personnel in preservation efforts
- Reliance on individual personnel to preserve ESI without proper guidance, training or supervision
- Information that is lost when individuals leave the organization
- Relevant data that is unknown to the organization
- Backup tapes that are incorrectly identified as "unavailable" when they are available or in offsite storage facilities, or are represented as being overwritten when they have not been
- The existence of large volumes of email on file servers and backup tapes that have been taken out of service but not yet overwritten

E-Discovery Risks in Regulatory Investigations

The most serious risk associated with an organization's response to a regulatory investigation is the inadvertent destruction of information, which a regulator may view as a failure to cooperate or, even worse, as a willful attempt to obstruct an investigation. Therefore, organizations must endeavor to preserve relevant ESI in connection with any such investigation. Keep in mind that regulators often have a variety of mechanisms available to them to enforce preservation obligations.

For example, there are harsh criminal obstruction of justice laws, both federal and state, that can apply when an organization does not preserve documents when responding to a regulatory investigation. The possibility of obstruction of justice charges for knowing or willful destruction of ESI is a powerful motivator in driving an organization to proactively manage and address the preservation and collection of ESI. In addition, regulators have used the record-keeping requirements of the Securities Exchange Act of 1934 as a means to ensure the preservation of documents relevant to an investigation.

The SEC has aggressively pursued violations of those record-keeping rules through enforcement actions, including violations discovered in connection with an organization's response to requests for production of ESI. Similar, but less comprehensive, record-keeping rules have been enacted for the accounting industry under the Sarbanes-Oxley Act, and have been created by Title VII of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act.

Best Practices for Managing ESI in Regulatory Investigations

Effective planning and appropriate disclosure is the key to satisfying regulators that an organization has complied with its preservation and production obligations. If a regulator is satisfied that an organization is attempting, in good faith, to comply with its request, the regulator may be more willing to negotiate limits on the preservation and production obligations to help the organization manage the costs and burdens of compliance.

Formulate a Preservation and Collection Plan. Prior to receipt of a specific regulatory request for production, identify key data sources for ESI and develop a plan for the proper preservation and collection of data from those sources, including custodian data, organizational data and data from disaster recovery systems.

Document Preservation and Collection Efforts. The best way to convince a regulator that appropriate steps have been taken to preserve and collect relevant data is to be able to explain to the regulator exactly what steps were taken. Carefully documenting the organization's efforts to implement its

preservation and collection plan will put the organization in a position to provide immediate and accurate answers in response to a regulator's questions.

Anticipate Second Requests. It is common for regulators to issue second requests for production after the initial production has been completed. It is good practice to anticipate the possibility of a second request and to consider during an initial review and production which data, if any, may be useful for later production in response to a second request.

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

Be Aware of Production Guidelines. Many regulators have specific guidelines for production. Compliance with such guidelines is presumed, and organizations and their counsel must be cognizant of them. Any burdens or challenges of meeting the production guidelines should be raised during the meet and confer with the regulator.

Negotiate. It is possible, and advisable in most cases, to negotiate the scope of preservation and production with a regulator. Keep in mind that regulators often have staffing or budgetary limitations, as well as time constraints, that impact their ability to review large volumes of data. Counsel for an organization should be prepared to discuss scope limitations on the preservation and production to the most relevant ESI, which may reduce the costs of compliance.

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

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

Please visit us at www.mayerbrown.com.

Electronic Discovery & Records Management

Tip of the Month

Why Information Governance Matters: Lower Costs, Reduced Risk and Better Business

Scenario

The chief executive officer of a large organization with multiple divisions and tens of thousands of employees across the United States is interested in minimizing the risk of lost records, reducing costs, and enhancing the ability of the organization's employees and customers to use the information and knowledge collected by the organization. The CEO asks each operating unit of the organization to update and enhance its records management policies and practices.

Proper Management of Electronic Records

In most companies today, 90 percent or more of the records being created are electronic. The overwhelming growth of electronic messages—email, instant messaging, texts, and twitter—and the likelihood that messages are stored multiple times on various media, makes the management of electronic records a critical business issue. How that information is managed has significant business, legal, and technology ramifications. However, from a records management perspective, the medium used to create, deliver, or store information is irrelevant; it is the *content* of a record that mandates how the document should be managed. Yet, in many organizations, the function of records management is still the realm of paper folders, physical file rooms, and dusty warehouses. As the amount of electronic information grows, the ability to manage that information, which is often very valuable to an organization, can diminish rapidly.

Presidential Memorandum on Managing Government Records

On November 28, 2011, President Obama issued a Presidential Memorandum directing all executive agencies to begin the process of reforming records management policies and practices.[1] Although the requirements of this memorandum apply only to federal agencies, these timely records management reminders are important for private companies and other non-governmental organizations as well.

Recognizing that "[i]f records management policies and practices are not updated for a digital age, the surge in information could overwhelm agency systems, leading to higher costs and lost records," President Obama ordered all heads of federal agencies to begin the process of reforming their records management policies and practices. The memorandum, in an effort to "develop a 21st-century

framework for the management of Government records," outlines a number of steps federal agency directors must now take, including:

- Within 30 days of the date of the memorandum, designate in writing to the Archivist of the United States (Archivist), which senior agency official will supervise the review process explained below; and
- Within 120 days of the date of the memorandum, submit a report to the Archivist and the Director of the Office of Management and Budget (OMB) that:

    - "describes the agency's current plans for improving or maintaining its records management program, particularly with respect to managing electronic records, including email and social media, deploying cloud-based services or storage solutions, and meeting other records challenges;
    - identifies any provisions, or omissions, in relevant statutes, regulations, or official [National Archives and Records Administration (NARA)] guidance that currently pose an obstacle to the agency's adoption of sound, cost effective records management policies and practices; and
    - identifies policies or programs that, if included in the Records Management Directive required by section 3 of this memorandum or adopted or implemented by NARA, would assist the agency's efforts to improve records management."

Lessons for the Private Sector and Non-Government Organizations

The President's memorandum, although limited in scope to federal agencies, nonetheless can serve as a reminder and inspiration to private companies, state governmental agencies, and other non-government entities of the importance of efficient, modern, and legally sound records management policies and practices.

- *Designate an official who is knowledgeable in records management practices*. Whomever is tasked with analyzing, updating, and improving the management of records should be familiar with the entity's current records management protocol, as well as more recent developments in the field, especially practices involving electronic records (including email and social media) and cloud-based services.
- *Ensure the proper allocation of resources*. Although a principal benefit of records management reform is long-term cost savings, entities will likely need to allocate resources in order to enact these money-saving procedures.
- *Familiarize senior management with records management requirements and benefits*. Records managers in private companies and non-governmental organizations can work to educate senior management on records management legal obligations, including data privacy and regulatory obligations, and the benefits of information governance to the bottom line and business efficiency.
- *Make information governance a priority for the entire organization.* The successful implementation of improved records management policies will cut costs, streamline the agency's information management system, and facilitate a more efficient and effective response to the demands of litigation.

- *Information and records management policies and procedures should be realistic, practical, and tailored to the circumstances of the organization*. No single standard or model can fully meet every organization's unique needs. Each organization should consider its own particular business needs, operations, IT infrastructure, and regulatory and legal responsibilities before putting in place a practical, flexible, and scalable records management policy.
- *An organization need not retain all electronic information ever generated or received*. This is especially important in today's world of email, instant messaging, text messaging, and multiple duplication of data for disaster recovery and other purposes. Absent a legal requirement to the contrary, an efficient records management policy should include programs that routinely delete redundant records and other data.
- *Ordinary destruction practices must be suspended as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigations, or audits*. Legal holds should be tailored to the legal requirements of the situation and informed by legal judgment. Moreover, effectively communicating and ensuring implementation of notice of a legal hold is an important component of an organization's records management policy.

In an era when a single smartphone, laptop or tablet computer can hold more information than some libraries, it is important that entities have effective and workable records management programs and policies. Knowing where and what records are kept, how to access those records, and when to discard them is a good way to start the process of developing and implementing a information governance program for the digital age.

For inquiries related to this Tip of the Month, please contact Anthony Diana at adiana@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com, or Aaron Chait at achait@mayerbrown.com.

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

Please visit us at www.mayerbrown.com.

[1] Mayer Brown LLP represents the National Day Laborers Organizing Network in a FOIA litigation against various government agencies in the Southern District of New York. As part of that representation, the government agencies' record-keeping practices for electronic records have been exposed as insufficient, as highlighted in a decision by Judge Scheindlin regarding the need to produce certain metadata for electronic records in response to a FOIA request. This case has been mentioned in the press as a leading driver behind this Presidential Memorandum.