The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 3 March 2011

Discovery – Law Firms

Basic Steps In E-discovery Continued: Knowing Where "Stuff" Is And Planning To Retain It

Mark L. Austrian and Martin Krolewski

KELLEY DRYE & WARREN LLP

This is the second in a series of articles intended to provide some thoughts on how to reduce costs and bring some rationality to e-discovery. We have advocated creating an overall e-discovery plan before litigation begins that might include the following: designated e-discovery teams; ESI systems analysis; record retention policies; trigger event guidelines; legal hold guidelines and forms; cloud computing requirements and social media policies. We have discussed the e-discovery team and triggering event guidelines in a prior article.[1] This article focuses on two critical components of an e-discovery plan: ESI systems analysis and record retention policies.

ESI Systems Analysis

Companies and their employees ought to know where their information is. But this often is not the case. In the *Intel/AMD* litigation, some Intel employees incorrectly assumed that their e-mails were being automatically archived, resulting in the automatic deletion of those e-mails and the loss of a significant amount of information.[2] The problem is that ESI gets dispersed and duplicated very rapidly throughout the company and the storage systems change over time. One solution is to create a data map describing the company's records by business unit, if appropriate, and specifying the various types of electronic media on which they are maintained. The data map could include: (1) active and dynamic servers such as file servers, e-mail and voice-mail servers; (2) data management systems such as backup tapes, financial systems and disaster recovery systems; (3) endpoints including desktops, laptops, cell phones CDs, etc., and (4) data hosted by third-party vendors such as payroll systems, and junk-mail-filtering services.[3]

Mark L. Austrian

Martin Krolewski

From a tactical perspective, the detailed information in a data map can be used by outside counsel to convince their opposition – or the court – that certain forms of ESI are too difficult or costly to access. For this reason, backup systems should be analyzed and cataloged, and facts should be gathered regarding what is backed up, whether the backed up material is available from other sources, where the backups are located, how backup media is rotated or recycled, and whether backup data is used solely for disaster recovery or is routinely accessed for so-called "convenience restores." To support any argument that the less active data is not readily accessible, this analysis should also document the costs associated with the accessing of such information, including the costs of data restoration and any hardware or software that may need to be acquired to access the data.

A data map will also facilitate the design and implementation of proper litigation hold procedures, which must be in place shortly after the threatened or actual litigation. Many recent cases stress that businesses must suspend ordinary procedures for the disposal of records, including emails and backup tapes, once there is reason to believe they are relevant to potential litigation. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc*., 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), is an often-cited example of the consequences of not knowing where all of the ESI is stored. Morgan Stanley was found to have violated its discovery obligations, primarily because it did not know where its discoverable information was located, and the jury awarded the plaintiff $1.4 billion in compensatory and punitive damages.

The data-mapping process should also review so-called "deleted" files, which while often difficult to retrieve can be relevant to litigation, such as by determining whether the business uses file recovery software that hides deleted files, or retains deleted email files outside any user-selected parameters. In addition, the business should identify and analyze repositories of potentially relevant "metadata," such as email log files and Internet histories. Potentially relevant "legacy data," e.g., data the business can no longer access because of software or hardware upgrades or replacements, should also be inventoried and analyzed.

The data map must remain current and relevant since digital storage growth and application upgrades seem constant and unrelenting. Data map maintenance can be

***Mark L. Austrian** is a Litigation Partner at Kelley Drye & Warren LLP. He serves on the Board of the Georgetown Law School's E-discovery Advisory Board, is a Member of the Sedona Conference Working Group on Electronic Document Retention and Production and teaches e-discovery at American University, Washington College of Law. **Martin Krolewski** is an Associate of Kelley Drye and has been active on numerous e-discovery matters.*

Please email the authors at maustrian@kelleydrye.com or mkrolewski@kelleydrye.com with questions about this article.

tied to existing processes that already deal with change management, such as IT project management processes and financial department purchasing processes. The data map could be updated with the sunset dates of any software version whose license expires or is superseded with a new version or product.

Document Retention Policies And Plans

A written records retention policy is a set of official guidelines or policies governing how documents will be managed, stored and destroyed. These policies may incorporate or attach particular disposition schedules for particular classes of documents. These should be created by legal counsel in consultation with senior management, as well as IT and records management personnel. Document retention schedules should not be based upon purely regulatory compliance but must use an approach emphasizing that many documents have significant business value. Not all documents have business value, only some of them. The key for workable policies is to provide some level of balance in how many and how long documents are kept.

The United States Supreme Court in *Arthur Anderson LLP v. United States,* 544 U.S. 696 (2005), confirmed that companies may design their own document retention policies based upon their own legal and business needs. This overall approach is documented in the safe harbor provisions of Rule 37(e). Consistent adherence to a document retention policy, in place before the litigation, allows counsel to explain why particular corporate records are not available. There is no presumption of "spoliation" with short retention periods. A consistently applied policy also reduces the risk that particular pieces of correspondence will be taken out of context when information surrounding the creation of that correspondence has been destroyed. A good retention policy also avoids the need to incur thousands, if not millions, of dollars, to search for millions of emails that have no particular value to the corporation.

The emphasis here is on "consistency," and if record retention policies are not properly communicated to company employees and not carefully monitored, this litigation benefit will evaporate. The policy should be clear and straightforward so that there cannot be any question as to whether it is understandable.

Finally, one of the criteria for judging whether reasonable steps have been taken when there is a claim of spoliation is the implementation of efficient records management systems prior to litigation.[4] The Sedona Conference® Commentary on Legal Holds (August 2007) *available at* http://www.thesedonaconference.org/content/miscFiles/publications_html), emphasizes the value of a document retention policy from this perspective:

> *Guideline 2*
> The adoption and consistent implementation of a *policy* defining a document retention decision-making process is one factor that demonstrates reasonableness and good faith in meeting preservation obligations.

A written policy may also protect the company where the legal hold is not put into place immediately after the trigger event pending discussions with opposing counsel at the Rule 26(f) conference. In *Olson v. Sax*, 2010 WL 2639853 (E.D. Wis. Jun. 25, 2010), a video had been destroyed after the trigger date pursuant to the company's regular document retention policy. Under those circumstances, the court refused to impose sanctions, since there was insufficient evidence as to bad faith.

We have generally recommended that the retention policy cover the following areas:

- *Define its Purpose*. Set forth the company's commitment to an effective document retention program that covers electronic documents and complies with the business and legal requirements, including document retention in the event of litigation.
- *Record Retention Goals*. Communicate what the company wants to accomplish (e.g. comply with legal requirements, delete unnecessary records, etc.).
- *Establish Policy Management*. Set forth the department with responsibility for overall management and its corresponding functions.
- *Create Management Administrative Responsibilities*. Decide how the program will be managed within particular business units.
- *Management and Employee Compliance Responsibilities*. Emphasize the need for employees to comply with the Policy and accompanying schedules and the need to follow litigation hold instructions.
- *Storage*. A general description of how the records will be stored.
- *Destruction/Deletion*. The need to follow a consistent practice.
- *Cessation or Record Destruction or Deletion*. Practices to employ once a legal hold is in place.

Companies may include or prepare a separate schedule specifying particular categories of documents with specific retention periods.

One of the main problems with document retention schedules involves making sure that employees comply, since this is often viewed as an unproductive nuisance and, for documents they deem important will engage in "underground archiving." One possible approach is to capture documents in an archive that automatically deletes documents after a prescribed period of time but gives employees the option of saving some important documents longer than the stated retention period by manually overriding the deletion period. Some individuals will do that for some documents. Most, knowing that they can retrieve older documents at some point in time, will forget. The result will be that most documents are deleted by the system, without the employees engaging in underground archiving.

Unfortunately, too often messages on document retention/deletion come across as the legal department dictating from the top of the proverbial mountain, telling employees how saving fewer documents is better (for legal, that is). Employees quickly tune out these messages. Good record deletion strategies do benefit legal, as well as IT, HR, business units and other departments. Perhaps most important, good retention and deletion systems can also benefit employees themselves.

It is also important to assess how much compliance there is with the current retention policy. The company should train employees on compliant retention and deletion. Once the program is launched, the retention program should be assessed. If the training did not accomplish its goals, then it should be modified. The company should implement ongoing monitoring to insure that the right documents are being saved and any given employee is not saving too much beyond the policy.

Conclusion

Many corporations have advocated the need to completely revamp our civil discovery system. Whatever the merits of their arguments, it is not going to happen in the short term. In the meantime, careful planning can reduce some of these corporate headaches.

---

[1] Austrian and Krolewski, *Basic Steps in Ediscovery: Creating the Team and Knowing When to Pull the Trigger,* The Metropolitan Corporate Counsel (January 2011).

[2] Keith Regan, *AMD Accuses Intel of Mishandling Evidence*, E-Commerce Times, Mar. 6, 2007, *available at* http://www.technewsworld.com/rsstory/ 56126.html.

[3] See H. Christopher Boehning, *Know Your Data,* New York Law Journal, (Nov. 5, 2007).

[4] See Report of the Advisory Committee on Evidence Rules (May 2007), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/2007-05-Committee_Report-Evidence.pdf.