

The Importance of IT Due Diligence

by David J. Kessler

Summary: *How can a company know that it is preserving all relevant documents if it does not know what documents it has and where they are stored?*

David would like to thank Christopher Coval for his help with this article.

As e-discovery becomes the hottest new (or, at this point, not so new) thing, everyone is talking about the recent amendments to the Federal Rules of Civil Procedure and the latest cases on metadata or spoliation or cost-shifting. Lawyers are being bombarded with calls from e-discovery vendors hawking the newest revolution in technology that will allow them to review a company's documents faster than ever. Vendors have the technology.

However, one part of the picture seems to be routinely neglected: IT system due diligence. Lawyers and corporations that neglect a thorough review of their computer systems do so at their own peril. While corporations and their counsel must understand the law, their obligations and the vendor technology at their disposal, if they do not understand their own IT system, they will not apply skills and knowledge in a cost-efficient or effective manner.

Why the Corporation's IT System is a Mystery, Even to the Head of IT

Anyone who has worked with computer systems would readily admit that IT systems are complex and difficult to understand. Yet lawyers and managers often delegate responsibility to review such systems to others without getting familiar with how the system really works. Counsel and business managers may feel they do not have any expertise in this area and leave it to IT personnel to understand the systems. Or they may feel that how a corporation organizes and maintains its electronic documents is a tertiary problem at best and that lawyers should focus entirely on the merits of their case and the litigation strategy. Whatever the reason, this practice can quickly undermine even the strongest and best cases. In general, just as counsel are not experts in computer systems, IT managers are not experts in litigation, preservation or discovery and may not give as complete or thorough an answer to lawyers' inquiries because they do not understand what is important. While the merits of any particular case are obviously important, if a corporation's preservation and collection of documents is haphazard because the lawyers do not understand how the corporation stores its own information, this can quickly provide leverage to the opponent and lead to weaker settlements or bad outcomes at trial.

For many corporations, their computer systems were not developed with the current configuration in mind. Computer systems are organic systems that evolve to meet the needs of their companies within the confines of personnel and financial resources. They are creatures of both rapid corporate and technology changes. While an initial plan may have been laid out for the company's IT system, this plan quickly became obsolete as the company's needs changed. Sometimes the plan is revised, or sometimes the plan is forgotten and honored only in the breach.

The Problem for Discovery

For lawyers and the corporations they represent, this creates challenging pitfalls in both litigation and document retention management. If lawyers recommend strategies and policies based on what the lawyers, and even management, believe (but have not verified) is happening within their company, then this advice can backfire and create discovery problems in future litigation. For example, it may be a company's policy that employees are provided only a set amount of memory for their email and are prevented from saving any email to their hard drives. However, this policy, or the technological restriction, may not have been implemented after a merger or the creation of the division. Counsel and management who make decisions regarding discovery based on the company's official IT and document retention policies, without investigating how employees are actually implementing them, may be shocked to find themselves inundated with unexpected data or worse, find out they missed whole chunks of data until late in the discovery process or trial. Every lawyer wants to avoid finding out from a witness in preparing for a deposition that he or she did not look at, review, produce or preserve certain files because it was not part of the policy or hold memorandum.

At this point, everyone has heard of cases where companies have been sanctioned for failing to preserve documents including *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.* and more. Obviously, not all of these sanctions were caused by the failure to conduct an investigation into a company's computer system. Still, how can a company know that it is preserving all relevant documents if it does not know what documents it has and where they are stored?

Beyond spoliation, parties and their counsel also have suffered in the courtroom for not knowing the powers and capabilities of their own computer system. (For example, see *Invision Media Communications, Inc. v. Federal Insurance Co.*) Counsel should not represent that a certain document cannot be produced because it was deleted under the document retention policy unless he or she is certain that is true. In the *Invision Media* case, the court sanctioned the plaintiff and its counsel for making representations to the court and opposing counsel without undertaking a reasonable investigation. In response to a document request seeking "all electronic mail communications sent or received by Plaintiffs during August 2001, September 2001 and October 2001," plaintiff's counsel stated that no email was available because, as a matter of policy, the company retained email for two weeks only. It was later discovered that plaintiff did possess responsive emails and the court found that:

A reasonable inquiry by plaintiff's counsel prior to responding to Federal's document request . . . would have alerted counsel that the plaintiff possessed electronic mail that fell within the scope of Federal's document request.

These problems are likely to become only more intense as the amendments to the Federal Rules of Civil Procedure take effect on December 1, 2007. With changes to Rules 16 and 26, there is a concerted effort to compel parties to discuss e-discovery early in litigation and to reach agreements about the scope of discovery. If counsel does not understand the possible scope of the corporation's computer systems, counsel will be ill prepared to reach agreements with opposing counsel or respond to the court. How can a lawyer effectively evaluate whether a proposed stipulation is reasonable or overly burdensome if he does not know how it will actually affect the IT system?

In addition, the amendments to Rule 26 create a two-tiered discovery system that may require lawyers to understand their client's computer system in order to respond to *any* requests for production. Under the new rules, parties are going to have the opportunity to object to the production of certain data from certain sources if it is "not reasonably accessible." However, lawyers will not be able to make this objection if they do not understand the system because they will not know what data, if any, on the system is "not reasonably accessible because of undue burden or cost."

Conducting Due Diligence on Your Own Computer System

The only solution for both the company and counsel is conducting a reasonable investigation into the corporation's own computer system. Counsel cannot rely on reports of how the system was set up to run or how IT staff thinks it runs; counsel should learn how the company's employees actually use the system. The keystone for all discovery obligations is reasonableness. Corporations and counsel are under no obligation to investigate every aspect of a company's computer system. They need to understand the corporation's computer systems well enough to preserve information that they reasonably believe is reasonably relevant to the litigation at hand. If the litigation would not involve a company's sales force or human resources department, then it is likely that counsel does not need to investigate how the computer systems in those departments operate. Moreover, even in business units that are involved in the litigation, counsel only needs to conduct reasonable diligence - understanding every aspect of the computer system or every idiosyncratic use of the system by every employee is not reasonable.

Strategic companies should enthusiastically support IT due diligence. Not only will it prevent nasty surprises in discovery and allow better litigation planning, but it will help mold better IT and document retention policies going forward. If a certain department is using disaster recovery tapes as an archive against company policy, then it may make business sense to invest in a proper electronic archiving system that is designed for long-term storage and retrieval of documents and prevents the inefficient use of disaster recovery tapes and the co-mingling of disaster recovery data and with information. This not only improves litigation planning and budgeting but also improves IT planning and budgeting.

One of the best ways to conduct IT due diligence is to talk to each of the key witnesses regarding how they create, store and maintain their electronic documents early in the process. Counsel should draft an interview sheet for each witness that not only covers the substance of what they know and how they are involved in the litigation, but also where they store documents. It is also useful by those departments to discuss with relevant departments the information created in the ordinary course of business. If counsel and the company know how *and why* information is created, the information will be much easier to collect and review.

When learning a company's IT system, it is normally best to interview not only the IT managers, but lower-level IT analysts and support personnel who regularly work with the business units relevant to the litigation. High-level IT managers are by definition dealing with more abstract and general problems than day-to-day managers who know what workarounds and ad hoc solutions have been performed to accomplish business tasks that may be very relevant to the current litigation.

One final recommendation: make friends with the company's IT personnel. Just as you try to understand how the business operates and the pressures exerted on individual decision makers within the company, the lawyer should learn how the IT system operates and the impact on the various IT personnel. Civil discovery puts tremendous pressure on IT systems and the people who run them. In many cases, the budgets and man-power for these departments are already stretched by the demands of the business, and discovery only adds to those woes. Opposing counsel and the courts may attempt to push computer systems to do things the systems were not designed to do; as counsel for the corporation the lawyer must understand and explain the limits of the system in detail to others. Friends in the IT department which can help the lawyer think outside the box or alert the legal team to problems it has not yet arisen.

Learning a company's documents and computer system on the back end - during the review for responsiveness, privilege and production in litigation - is an inefficient and expensive method of performing discovery. If lawyers do not know anything about the documents they are reviewing until they have started their review, not only are they bound to make early mistakes, but it is hard to pinpoint documents and maximize their resources to review the most important documents first. Corporations and their counsel should not rush to identify, collect and process documents simply to meet the deadlines imposed by the courts and the rules. Rushing to place documents in front of

reviewers leads to documents being reviewed more than once and may actually slow down review. More investment in time and energy in the beginning of the review - learning about a company's documents and computer system - not only avoids problems with discovery, but saves time and money for lawyers and their clients.

David J. Kessler is a partner at Drinker Biddle & Reath LLP specializing in e-discovery and data management as well as IP litigation. He regularly counsels clients regarding record retention policies, litigation preparedness and e-discovery risk management. He can be reached at david.kessler@dbr.com or (215) 988-2486.

Copyright 2007, SourceMedia and DM Review.