

# **North Chamber CIO Breakfast**

**July 24, 2008**

**Don't Become a Victim of E-Discovery:**  
Understanding how careful planning and communication can improve  
your company's position in the emerging world of electronic litigation

**Tony Avey**  
**Brendan McBride**  
**John Saba**



**Prichard, Hawkins, McFarland & Young**  
10101 Reunion Place  
San Antonio, Texas 78216  
210.477.7400  
[www.phmy.com](http://www.phmy.com)

**Don't Become a Victim of E-Discovery:**  
**Understanding how careful planning and communication can improve your  
company's position in the emerging world of electronic litigation**

**Tony Avey, Brendan McBride, John Saba**  
Prichard, Hawkins, McFarland & Young

Nobody wants the intrusion of litigation into the day to day affairs of their business. But the reality of the modern business world is that sooner or later, your company is likely to find itself in litigation at some point, and high stakes litigation may even decide the ultimate fate of your company. Much of modern business takes place through emails, computer files and databases. Slowly but surely, the litigation world is catching up to the world of modern business, developing new rules governing the way in which lawyers obtain electronically stored information from the opposing side for use in a case ("e-discovery"). Like any other litigation risk, success in controlling risks related to e-discovery depends on understanding the rules, assessing the risk, developing a proactive strategy to try to prevent problems, and having a plan in place to solve problems when they arise.

Starting back in December 2006, new rules were enacted as part of the Federal Rules of Civil Procedure to better define the parties' obligations in seeking and responding to civil discovery of electronically stored information (or "ESI"), including emails, documents contained in application-generated files, databases, and "metadata" for all of these. The new rules make clear that electronically stored information is definitely subject to discovery in civil litigation. This potentially includes everything from obvious electronic "documents" such as emails, word-processed files, and spreadsheets, to information contained in back-end databases, source code, computer data models and metadata (which is discussed in detail below).

Unlike more defined compliance or regulatory requirements for data management, like HIPAA or Y2K, there's no point at which a company can breathe easy, confident that for the most part it has done what it needs to do with its data management to minimize risk. Not only are these new rules evolving as courts across the country are learning to apply them to real-world problems in e-discovery, but problems may be difficult to predict, as it's often not until well after litigation is underway that it becomes apparent that a missing email or Excel document is or would have been the key to a multi-million dollar case.

The overriding purpose of the new rules was to give litigators and judges more concrete guidance as to what can reasonably be expected as part of the discovery of electronically stored information and the procedures for going about obtaining it. Like any new rules system in its early stages, it is in a state of constant flux as courts around the country wrestle with how to apply these general rules to the many unique situations that arise in actual litigation. Nonetheless, a solid understanding of what the rules are and what they aim to accomplish is the first step in understanding how best to control e-discovery risks.

Here are some tips and information about how – given the purpose and scope of the e-discovery rules – planning, coordination and communication can help control the company’s risks, and improve the outcome of litigation.

***The E-Discovery Conference:  
Identify the Data Potentially At Issue Early On and Make a Plan.***

The new rules require the parties to meet very early on to discuss potential issues related to e-discovery. At these e-discovery conferences, the parties’ lawyers are expected to agree to the logistical plans for searching, retrieving, preserving and producing electronically stored information. This will require someone familiar with the technical aspects of the company’s data management to be in a position to clearly inform litigation counsel - very early in the case - of what ESI is and is not available, the potential problems with accessing and searching the company’s systems for potentially relevant ESI, and the potential costs involved, so that all of the potential problems and advantages available to the company can be evaluated and considered as part of the initial e-discovery conference.

Necessarily, the company will need an accurate profile of all of its electronically stored records readily available, and someone with sufficient knowledge and technical expertise available to answer specific questions about the nature and location of potentially discoverable electronic records, the file formats, search capabilities, restrictions on access, potential costs both directly and in terms of manpower, and metadata.

The company’s success in setting up a workable e-discovery strategy that minimizes risk, costs and intrusion will largely depend on how well the company has prepared to describe its system and capabilities to its litigation attorneys, so they can negotiate reasonable schedules and limits for production of ESI. A company without such a proactive, comprehensive approach will likely find itself running afoul of the courts, missing crucial documents in its production, trying to manage spiraling costs, and solving major problems at much greater risk, stress and expense, rather than preventing them.

The parties are also required to meet about the preservation of ESI at this initial e-discovery conference. So in addition to having a plan for educating counsel about your electronic resources, needs and limitations, the company should have a plan in place for preserving records potentially relevant to anticipated litigation and a process in place to communicate to all company personnel who have access to potentially discoverable ESI (including electronic files and emails that reside on desktop computers, laptops, PDAs and other devices issued to employees), to preserve these records. The company neither wants to be in the position of missing the key document to its case because it was not preserved, nor in the position of explaining to a judge why there was no procedure in place to preserve what your opponents are now claiming was the “smoking gun” document (and you can’t prove otherwise, because you can’t find a copy).

The reality is that oftentimes the outcome of major litigation is determined by what occurs in discovery. This is a place where careful planning, coordination and communication can make a real difference in the results of the case(s).

***“Reasonably Inaccessible” Electronic Data:  
Know Where It Is, And Be Prepared to Defend Your Decision Not To Produce It.***

The rules contemplate that sometimes ESI may be so difficult or expensive to access and produce that it substantially outweighs the practical need for the information in the litigation. In such instances, a party to litigation must understand when certain electronic data is “reasonably inaccessible.”

Some of the relevant considerations are: where the ESI is stored such that the hardware or software needed to access it is obsolete; where it is stored in such a fashion in such a volume that searching it and narrowing it down to potentially relevant information is so costly and time-consuming as to make it practically impossible (such as costly searches of thousands of backup tapes); where the media on which the ESI is stored is inaccessible due to damage; where the data is duplicative of other data that is already searched and produced; the requesting party’s own access to the same or substantially the same data from some other source; and, the significance of the information to the issues in the case.

The company should be aware of some of these unique challenges presented by its data management systems, archives and other repositories of electronic information. As with other issues, the company should be prepared very early on in a case to explain to its litigation counsel when such challenges are present, so that they can be taken into consideration as part of the initial e-discovery conference and hopefully resolved as part of the initial agreements.

If, after the initial e-discovery conference, a claim of reasonable inaccessibility remains unresolved, the burden is on the party whose ESI is sought to be produced to demonstrate that the information is “reasonably inaccessible.” If the party seeking the information successfully shows there is “just cause” for why the evidence should be produced, the court may then order its production.

Therefore, in addition to having a plan in place to identify potential issues with reasonably inaccessible data, the company should also be prepared to be able to present evidence of the technical, logistic problems justifying the conclusion that a repository of data is not reasonably accessible and to give some sort of specific quantified guidance as to the likely costs involved, where cost is an issue.

***Inadvertent Production of Privileged/Confidential Information:  
Minimizing It, and Controlling Its Effects When It Happens.***

Repositories of electronic information may contain information that is protected from discovery under a privilege. For example, emails might involve communications between company officials and the company's attorneys for purpose obtaining legal advice, or documents may contain information of a highly confidential and proprietary nature sufficient to justify withholding them as trade secrets. The larger the volume of ESI discovery, the greater the chances that some important, privileged materials might be inadvertently produced. This risk is particularly acute with regard to ESI because the sheer volume of information involved often makes it practically very difficult for attorneys to carefully review all of the electronic data to make sure it does not contain privileged information. The new rules, along with the parties own agreed "clawback provisions" to be determined as part of the e-discovery conference, are designed to reduce the potential damage when privileged information is inadvertently produced, but allowing the producing party additional leeway to "clawback" the privileged information provided it acts diligently after discovering the inadvertent production.

The company can help reduce the potential risks of such inadvertent production by having a plan in place for identifying where in its data repositories it is likely to keep information that would be categorized as trade secrets, attorney-client communications, and attorney "work product" (information that would reveal the work or thought processes of attorneys working for the company, or agents for attorneys such as legal assistants, risk managers and investigators).

***Stay in the "Safe Harbor":  
Document Retention Policies and the Duty of Preservation.***

Of all the challenges posed by e-discovery, the one most likely to have a substantial intrusive effect on the day-to-day management of business data is the rule governing the preservation of potentially relevant ESI while litigation is pending. Fortunately, the rules contemplate the practical problems facing a company in trying to preserve potentially relevant evidence and yet still run a business.

The new rules provide limited protection from being "sanctioned" (ordered to pay fines or the other side's attorneys' fees for discovery abuse) for parties who, in "good faith" and the ordinary course of business, have disposed of potentially discoverable ESI. The rule reads as follows: "absent exceptional circumstances, a court may not impose sanctions as the result of the routine, good-faith operation of an electronic information system."

The apparent intent of this rule is to make some safe harbor for ESI lost as a result of routine purges according to an established and consistently followed document retention policy, such as policies for deleting old e-mails, or recycling storage backup and

other media. To ensure that the company is best situated to take advantage of this safe harbor, make sure that the document retention policies are clear, and written, and that they are consistently followed for all documents - not just matters in litigation. Without such a policy, the risk of monetary sanctions by a court goes up dramatically.

Furthermore, the rule offers no safe harbor to a company that fails to preserve records by issuing appropriate litigation holds for relevant ESI, once the company reasonably should have anticipated a matter was likely to result in litigation. The company is on notice and must issue directive to preserve potentially relevant records once litigation is reasonably foreseeable. This is another area where careful planning and communication can avoid potentially disastrous results, and where small mistakes by employees not properly instructed can potentially cost the company millions.

### ***The Hidden Dangers of "Metadata"***

The rules treat "metadata" just like it does any other relevant ESI. It is not exempt from production, it should be preserved, and it may contain all sorts of information that the company should be aware of before production. The comments to the new rules define "metadata" as "information describing the history, tracking or management of an electronic file ... [that is] usually not apparent to the reader viewing a hard copy or a screen image."

Metadata for an electronic file may contain such information as who authored a document and when, when the document was created, last accessed, last edited, last printed or last saved, the word and character count in the file or document, or the structure of the document (numbers and name of pages in a spreadsheet for example), file system location, the template used to create the document and, depending on the type of file and the application used to create or modify it, a wide variety of other information. It can also include things like the html or other code behind a webpage, "cookies," or possibly even database field entries for a file or document management system; even though such metadata is not contained within the individual files themselves.

Thus, metadata presents three potential problems for a company in litigation. First, it presents the potential problem of inadvertently producing information the company might not be aware it is producing, as metadata is not readily apparent from the ordinary viewing of a document or other electronic file. There have been and will be major cases that revolve around information discovered in metadata.

Second, metadata presents unique problems with preservation, since much of the information contained in the metadata can be changed merely by the act of accessing or printing a file. To the extent possible, the company should include as a part of its policy for litigation holds of documents, instructions to employees not to alter documents subject to the hold.

Third, metadata presents potential production issues. Obviously, the metadata stored as part of the electronic files themselves (such as author, last edit data, title information, etc. in a MS Word or HTML file) are automatically produced when an electronic copy of a file is produced. However, not all metadata is included in the file. The company may have a document management system, for example, hosted on a database, that contains information about the tracking and sorting of the documents that are being produced. It's not clear yet whether such information is also required to be produced as "metadata." Furthermore, to the extent that ESI is produced in a printed out format, it would likely not contain the metadata and some arrangements would have to be made to provide the associated metadata for each file.

***Planning and Communication:  
Don't Be an E-Discovery Victim***

If there is one overall lesson to take away from the emerging world of electronic discovery in litigation it's this: problems are much easier to prevent than to solve. It is better to have a carefully thought out plan for understanding the potential advantages and risks your company faces in e-discovery, written policies for preserving documents and issuing litigation holds, and a plan for communicating with litigation counsel on the technical and practical issues potentially implicated should the company find itself mired in an e-discovery battle.