

Electronic Discovery  
The New Elephant in the Room

John M. Sier, Esq.  
Thomas D. Esordi, Esq.

No one wants to be sued and few companies or individuals willingly elect to pursue litigation in the federal courts. However, litigation is not always a voluntary process, and if you are being sued or receiving a subpoena, there is a particular issue that may impact your case and your future: electronic discovery. With the recent amendments to the Federal Rules of Civil Procedure that became effective December 1, 2006, governing the discovery process in federal court litigation, all companies--and even individuals--need to be aware that electronically-stored information ("ESI") is becoming a key part of the litigation - even if you are not a party to the lawsuit.

As everyone knows, electronic communication and storage devices have become so common that much business communication and many transactions never actually reach the paper medium. Between electronic mail, project websites, text messages, instant messaging and other forms of digital communication, there has been an exponential growth in the information exchanged electronically in addition to the paper. This proliferation of communication and storage devices has created a surfeit of information for lawyers to mine during litigation. In fact, the exponential growth in available information quickly overwhelmed the former procedural rules in place despite several modest amendments. Rather than taming the paper tiger, the new rules now seek to control the "electronic elephant."

The amendments were driven by the major distinction between paper discovery and ESI. Paper documents or tangible storage media are inherently static; once a document is created, the contents of the document will not change or impacted by the passage of time. ESI, on the other hand, can be changed by the mere fact of opening the particular file. ESI in many organizations is continuously being changed through routine operations of the computer systems. Plus, some of the ESI files contain hidden "metadata," which provides detailed historical information about the history of that particular file including the author, date of creation, revisions, concealed formulas and other matters. Many times, this metadata is as important as the information in the file. Over the last few years, several court decisions were issued attempting to provide some clarity to the process. The committee charged with amending the rules held several public hearings and received commentary from various participants in the litigation process and ultimately issued the proposed changes to the rules that have now been adopted. The following is a brief description of how the rules have been changed.

**Scheduling and Planning.** The rules have been amended to assist both the parties the court and preparing for litigation with the use of electronic discovery. The new rules encourage the parties to discuss electronic discovery at the very outset of the case. Businesses must now be aware that they will need to immediately disclose the identity of key individuals within their organization who are best equipped to identify the maintenance and flow of ESI. These individuals need to be familiar both with the organization's network and information system architecture as well as the universal operation of the business together with the role ESI plays in the day to day processes. Careful selection of these individuals is critical since they will be providing this information to the other side and likely to various consultants.

**Discovery and Duty to Disclose.** In the past several years, ESI has grown increasingly significant in business disputes, but the rules governing the discovery process didn't specifically address either parties' rights or obligations relative to all of the electronic information. With ESI being brought front and center, the parties need to identify and disclose the ESI that exists pertaining to the issues in the litigation. With these changes in the rules, businesses must investigate the ESI issues simultaneous with the investigation of the substantive issues in the litigation. The businesses also must understand how ESI may affect those claims and defenses.

**Reasonably Accessible Information.** Recognizing that the ESI may be located in several places and in several formats, the rules were supplemented by a completely new provision addressing unreasonable costs that may result from requests for multiple forms of the same information. Parties may argue that certain types of ESI is “not reasonably accessible because of undue burden or cost”. However, the party requesting that information may demonstrate good cause to the court in an effort to obtain the requested ESI despite the objection of the producing party. The court may order that the ESI be made available upon certain conditions including allocating the cost of making the ESI accessible. According to many states’ laws, a company is under an obligation to retain ESI that is material to an actual or potential lawsuit to which it may be a party. Designing and implementing a policy to capture and segregate that type of ESI could substantially limit potential exposure to sanctions or other court-imposed penalties for failure to preserve ESI in an accessible format.

**Conference Planning.** The amended rules direct and encourage parties to discuss discovery of ESI during the initial discovery planning phase. While there is no precise formula for this planning, the rule requires the parties meet as soon as practical and no later than 21 days before the initial scheduling conference; this conference could take place within a few weeks of the filing of the lawsuit. At the conference, the parties must develop a plan addressing the form in which the ESI will be made available and the steps that will be taken to preserve any applicable privilege. Information Technology specialists will be involved from the very beginning of the litigation. Diagrams of data retention and information flow will assist in clarifying the company’s position during these discussions. The parties must also immediately consider which aspects of these activities will need to be outsourced in order to preserve data integrity and to eliminate the potential for inadvertent destruction or corruption of data.

**Confidential Information.** The production of paper documents was typically delayed by the need by the lawyers to review the documents to remove those that were protected by the attorney-client privilege from being produced. The sheer quantity of the ESI that is available and being produced precludes the ability to conduct an effective privilege review. As a result, the production of ESI generates an increased risk of inadvertent disclosure of privileged or confidential information. The rule amendments allow for belated assertion of the attorney client privilege through agreement of the attorneys for the parties. Sometimes called a “clawback” agreement, it allows the parties to retrieve privileged information that was inadvertently produced. A business can limit this potential risk factor by segregating protected or privileged information either on separate servers or in a manner that identifies the privileged or confidential information.

**Interrogatories.** When it relates to paper discovery, a party is able to answer an opponent’s written questions by referring the opponent to records maintained in the manner that they were kept in the ordinary course of business. You can also refer the opponent to the ESI as it is kept, but the ramifications of that can be significant. The other option is to produce the ESI that specifically responds to each question in the interrogatories. Businesses that have and consistently implement data retention procedures will substantially increase their ability to respond that way.

**Preserving Electronically Stored Information.** With the ability to obtain ESI during litigation comes the requirement to preserve it. Even prior to these specific amendments, courts became less willing to tolerate destruction of ESI. Businesses must have in place the ability to put in place a “litigation hold” so that ESI is not destroyed or modified. This topic as much as any other places the legal requirements of preserving ESI for a potential lawsuit at odds with the Information Technology preference to store as little data as possible so as to maximize network performance and efficient use of resources.

**Form of Production.** The requesting party may now designate the format in which the ESI is to be produced; if the requesting party has not designated a format, then the producing party can decide the format. As with any legal decision, businesses must understand the potential pitfalls of producing ESI in a particular format. Choosing the format can be as important as the information to be produced. Full knowledge of the business’ capabilities may place it at a huge advantage during discovery by protecting certain information and reducing costs that may be associated with the production.

**Safe Harbor.** The amended recognize that not every business is designed to anticipate litigation, so the rules allow for some limited protection to entities who have and implement ESI policies. A court may not impose sanctions if the failure to provide ESI is because the information has been lost as a result of the routine, good-faith operation of an electronic information system. However, this is a very limited protection. It only extends to routine data management carried out in good-faith and does not prohibit the court from requiring the party from taking on additional obligations such as responding to further discovery and producing additional witnesses. In order to take advantage of this amendment, it is imperative that the business maintains information in an appropriate manner. This may include suspension of ESI destruction processes and protocols and implementation of the “litigation holds.” While “good-faith” is not defined, businesses that develop specific destruction schedules that relate to normal business operations; designate a records custodian or ESI management team; and, educate employees on company policies have a far better chance of being protected. This is likely to be one of the heavily litigated provisions of the amended rules precisely because the stakes can be enormous. If a court finds that ESI has been destroyed and the safe harbor does not apply, then the court could allow the other party to argue to a jury that the data was destroyed because it would have been harmful, and the court could instruct the jury to that effect. Thus, relatively innocuous data becomes much more ominous simply by virtue of the fact that it no longer exists.

**Subpoenas.** The amendments make it clear that subpoenaed third parties are now obligated to produce ESI as well. While the rules make it clear that a subpoenaing party may not place undue burden or expense on the subpoenaed non-party, the obligations of the subpoenaed entity now mirror those identified above.

Here is a short checklist to assist in maximizing the benefits of the amendments to the Federal Rules:

#### **Personnel.**

- ✓ Identify individuals who have knowledge of data retention policies and procedures as well as a full understanding of the operations of the business.
- ✓ Identify individuals who can describe the company's ESI retention policies as well as justification for such policies.
- ✓ Identify outside vendors that can assist in the following:
  - Creating retention policies that are based on potential litigation scenarios rather than the companies IT capabilities.
  - Meeting litigation hold requirements and proper maintenance of stored information upon notification of potential litigation.
  - Identifying formats in which documents may be produced to maximize cost efficiencies.

#### **Information Retention.**

- ✓ Maintain diagrams describing the complete workings of your IT infrastructure and network architecture.
- ✓ Document any changes in software use.
- ✓ Create backups uniformly and document of who is responsible for creating them and where the backups are located.
- ✓ Create a retention policy that is based on business operations and reasonable retention periods rather than limitations of your computer systems.

- ✓ Document where ESI may be stored outside of a usual server such as employee desktops, laptops, portable devices and removable storage media.
- ✓ Document employee training on proper and uniform retention of ESI including compliance with litigation hold requirements.
- ✓ Segregate and secure archival media.
- ✓ Segregate and secure privileged information.

## **Conclusion**

The amendments to the rules will take several years to fully understand, but over time the rules will be considered no more onerous than the current rules relating to paper discovery. Many vendors are viewing electronic discovery as a new market for generating substantial revenues, and several vendors are already advertising their skills in retrieving hidden, deleted or even destroyed data. It's not a pleasant process, but it can be brought under some level of control as long as the business engages in some planning before the lawsuit or subpoena arrives.

*This article is for general information only and does not constitute legal advice. In the event that you have a specific question, please consult with an attorney.*

DET02\1160446.02