## *Compliance – Legal Service Providers*

# How The New Federal Rules Will Likely Change eDiscovery Practice

**John Patzakis**

GUIDANCE SOFTWARE, INC.

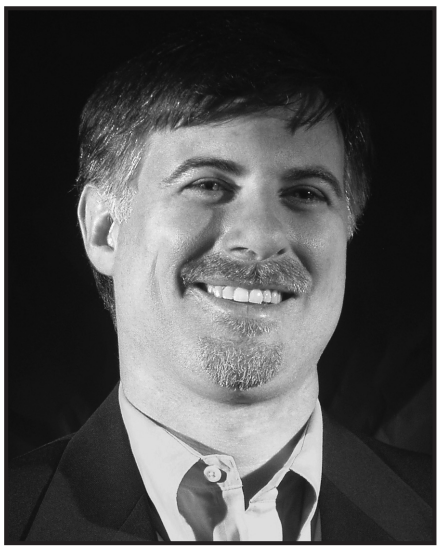
The amendments to the Federal Civil Rules of Civil Procedure will, barring unexpected intervention by Congress, take effect December 1, 2006 to specifically address the unique challenges of electronic discovery. The amendments will modify the existing rules in a manner intended to further highlight the importance of and provide a more established framework regarding electronic discovery. While many previous articles and notations detail the various amendments, the unanswered questions involve the procedural and operational adjustments large organizations and their counsel will likely undergo in order to adapt to the amendments. This article will discuss the practical effects of these rule changes and how they promise to impact existing practices concerning the discovery surrounding electronic data.

The likely impact of the amendments involves both intangible effects and more concrete operational changes. From a psychological standpoint, the Federal Rules of Civil Procedure is not often amended, and when it is, the entire legal profession, including the judiciary, obviously becomes keenly aware of such a development. As such, while eDiscovery has always fallen under the general purview of the current discovery rules, the amendments now specifically address electronic evidence discovery and provide standardized terminology and a clear framework. For instance, Rule 34 now defines computer based information and other digitally stored data as "Electronically Stored Information" (ESI). The ESI definition has already permeated the vernacular of key judges and legal pundits.

Consistent and uniform terminology and framework should result in a more consistent and uniform approach by the courts to ESI discovery. The new amendments send a clear message of standardization and inevitability surrounding ESI discovery. Everyone is on notice, and any uncertainty regarding the overall importance of ESI is removed. As such, ESI discovery practice will only increase and become part of almost all federal civil litigation.

In terms of more specific operational impact, a consistent theme throughout the amendments is one of a *de facto* requirement for large organizations to adopt a systemized internal process to address inevitable ESI discovery. This theme of systemization is steeped in three key elements of the amendments: The early attention requirements, the native file production requirement for ESI, and the safe harbor rule for deleted data in the normal course of business.

One of the most important aspects of the pending amendments is that they direct attention to electronic discovery issues early in the litigation process. For instance, the amended rules require that relevant electronic evidence be identified, preserved and disclosed at the initial outset of the litigation. As noted by the Judicial Conference in their September 2005 comments: "The proposed amendments to Rule 16,



**John Patzakis**

Rule 26(a) and (f), and Form 35 present a framework for the parties and the court to give early attention to issues relating to electronic discovery, including the frequently-recurring problems of the preservation of the evidence…"

The preservation element is particularly critical. Courts are increasingly holding parties to a stricter standard concerning the preservation of ESI and the amendments and their corresponding comments strongly emphasize the importance and duty to properly preserve ESI. The comments to Rule 26(f) note "[t]he volume and dynamic nature of electronically stored information may complicate preservation obligations...Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes." As such, under these new Rules, litigants will face a much higher likelihood of court sanctions if they fail to properly preserve relevant ESI at the outset of the litigation.

In order to properly identify, preserve and disclose relevant ESI, large companies are establishing a highly operational and systemized process to address ESI requirements as a standard litigation practice with each case, instead of a more reactive and *ad hoc* approach. The traditional "wait and see" approach to eDiscovery – where companies and their counsel often defer addressing ESI until its production is demanded by their opponent – results in a disjointed approach to ESI typified by hurried outsourcing or other non-systemized collection and preservation efforts that greatly increase cost and risk. However, such practices are no longer sustainable under this new framework. Only with an integrated, systemized and efficient internal process to routinely identify and preserve relevant ESI at the outset of each case will organizations be able to establish reasonableness in the eyes of the court.

Another key "systemization" element of the Amendments involves the provisions for the production of ESI. Rule 34(b) is amended to supply a procedure for specifying and objecting to the form of production of ESI. Under new subsections 34(b)(ii) and 34(b)(iii), the default form for producing electronically stored information is that "in which it is ordinarily maintained [or] reasonably usable." It is widely expected that parties will request that ESI be produced in native file format, which is generally how the data is ordinarily maintained and is the most usable format.

Additionally, numerous recent decisions hold that file metadata contained within ESI must also be preserved and produced, (*see, Nova Measuring Instruments Ltd. v. Nanometrics, Inc*., 417 F.Supp.2d 1121 (2006 N.D.Cal), *In re Verisign*, 2004 WL 2445243 at *1 (N.D.Cal.2004) (upholding discovery orders requiring production of documents in native format with metadata as not clearly erroneous: " '[t]he electronic version must include metadata as well as be searchable' "). See also *In re Honeywell International, Inc*., 230 F.R.D. 293, 296 (S.D.N.Y.2003). When ESI discovery is outsourced and not systemized, it is difficult to properly preserve and produce ESI in its native format with its metadata intact.

Outside consultants that handle their client's ESI will typically process the data in several stages to filter, de-duplicate and format the ESI for attorney review. Such processing is necessitated by an inefficient and non-systemized collection and preservation process that results in significant over-collection. In addition to being expensive, this processing often results in the loss of metadata and the conversion from native format to an image or .pdf format. An internal and systemized process can better preserve and produce ESI in its native format by utilizing enterprise technologies that enable more efficient and targeted data collection as well as review tools that support native file review and production.

Finally, the "safe harbor" rules are also a key "systemization" element of the new amendments. Subsection 37(f) is added which states, in full, "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system." The Advisory Committee Notes explain that ordinary computer use necessarily involves routine alteration and deletion of information for reasons unrelated to litigation.

However, in order for a party to establish that the deletion of ESI resulted from the routine and good faith operation of their electronic information system, the party must be able to demonstrate the existence of an established, well-documented and systemized electronic records management process. This process must be effectively tied into the party's litigation readiness plans, so that litigation holds are effectively executed. Again, this is impossible without a well-planned and established system-wide process. As with each of these elements of the new rules discussed above, the more established and systemized the process to preserve, collect and yes, delete ESI, the more reasonable and defendable the process will be seen in the eyes of the court.

So to address these challenges and the reality of the new framework, large companies are looking to bring much of their eDiscovery processes in house. A common new hire at Fortune 500 legal departments is a deputy general counsel exclusively dedicated to eDiscovery and records management. Their mission is to get the organization's eDiscovery and records management process in order, reduce risk and reduce costs. For large organizations, eDiscovery costs and associated risks are spiraling out of control. With a process that is largely outsourced, a major corporation can expect to incur tens of millions of dollars in out-of-pocket costs annually, mostly in the form of outside consultant fees to collect and process data. However, as much of the expense associated with a non-systemized eDiscovery process is incurred in the collection aspect of the investigation process, a global and systemized approach enables both cost savings as well as improved ability to comply with the amended Federal Rules.

The traditional and non-systemized approach to electronic evidence discovery involves a highly manual process to gather immense sums of data and then load that data onto a system that allows for searching and processing. This approach results in ever-increasing costs as the volume of data within a corporation grows. For instance, without enterprise computer investigation technology, collecting files from hundreds or even thousands of computers distributed across multiple locations must be performed manually. With no means to triage and filter out irrelevant data, the collection is overbroad, with a great deal of irrelevant data aggregated into a central database where it is then finally processed and searched. Metadata is lost in process and files are migrated into non-native format.

By providing for effective, customized and manageable system-wide searches of distributed workstations and servers throughout the global enterprise, a more targeted and presumptively relevant data set is returned to a centralized location in an automated fashion. Additionally, this technology enables the live and remote analysis and collection of evidence over a network from a centralized location in a sound and non-invasive manner and thus does not disrupt operations. This capability greatly reduces risk by providing a highly defendable process and reducing many of the pains and liabilities associated with a broken eDiscovery process.

Establishing a defendable process is a critical element of compliance as opposing counsel are now routinely seeking to capitalize on the eDiscovery struggles of large corporations. Claimants' lawyers in particular seek to distract the defense with "litigation within a litigation" allegations of spoliation or lack of due diligence in complying with eDiscovery requests. Plaintiffs seek to gain a significant advantage by obtaining evidentiary sanctions, petitioning the court for an order allowing their own experts to investigate the corporate defendants' systems, or otherwise driving up the cost of litigation by forcing costly and overbroad computer evidence investigations. With the new Federal Rules framework, these tactics are only going to increase.

An established enterprise investigation capability can be a powerful shield against these tactics, as the software is built upon the same processes and technology as those relied upon by top law enforcement agencies for their computer investigations. (*See*, eg, *Sanders v. State*, —- S.W.3d —, 2006 WL 561853 (Tex.App.-Waco) *[The Court notes that "EnCase is the field standard for computer forensics investigation."]*) Such a solid foundation of credibility and reliability provides a highly defendable and diligent process to establish compliance with the courts in eDiscovery matters. In light of the new Federal Rules' clear and consistent emphasis on the importance of properly preserving and identifying relevant ESI, large organizations can ill-afford not to have such a scalable, systemized – and thus defendable – process in place.

***John Patzakis** is Vice Chairman and Chief Legal Officer of Guidance Software, Inc., www.guidancesoftware.com.*

***Please email the author at legal@encase.com with questions about this article.***