A NEW YORK LAW JOURNAL SPECIAL SECTION

INVESTIGATIONS & COMPUTER FORENSICS

WWW.NYLJ.COM TUESDAY, MAY 29, 2007

ART BY NEWSCOM

Federal Rules Amendments

Traps for the unwary ahead, so get your ESI house in order.

BY JASON PICKHOLZ
AND STEPHANIE GIAMMARCO

AS THE WORLD keeps getting smaller and smaller, the amount of electronically stored information (ESI) keeps getting larger and larger. Recent amendments to the Federal Rules of Civil Procedure (Rules) endeavor to reflect this reality. But do these new federal amendments make the jobs of corporations and their lawyers easier by circumscribing the issues and establishing a universally applicable rubric to guide data management and discovery? Or do they give rise to unforeseen ambiguities that put outward pressure on the very parameters the amended Rules hope to establish?

The changes to the Rules pose challenges in a variety of areas, from textual vagueness, to business and technical operational issues, to legal strategic implications. To avoid surprise and potentially costly missteps, a corporation would be well advised to consider these challenges in advance and to implement a proactive team-based approach toward understanding and organizing its ESI and the systems on which it resides.

Procrastination Is Hazardous

The amendments to Rule 26(f)(3) require counsel to discuss "any issues relating to disclosure or discovery of electronically stored information," including preservation issues, during a pre-discovery conference. For practical purposes, the parties will typically have one to two months from service of the complaint in which to hold the Rule 26(f) conference.[1]

In order to effectively discuss issues relating to ESI at that conference, counsel needs to first understand the corporate client's ESI.

Under the widely-recognized *Zubulake* line of cases, not only the corporation, but also its "counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold.'"[2] If the company waits to satisfy its obligations under Rule 26(f)(3), it may find itself in the position of having to analyze its ESI systems and policies for the first time during the same period that it is evaluating the complaint, attempting to determine relevant facts, trying to retain litigation counsel and consultants, and drafting its own answer or motion to dismiss the complaint.

This may require a significant diversion of corporate time, resources and personnel to ESI issues, and can be extremely costly and disruptive to daily business activities, especially where the organization had little or no advance warning of the filing of the complaint.

Anticipating the 'Litigation Hold'

Rule 26(b)(2)(B) requires a party to identify sources of ESI that it claims are not reasonably accessible, in addition to what is accessible.

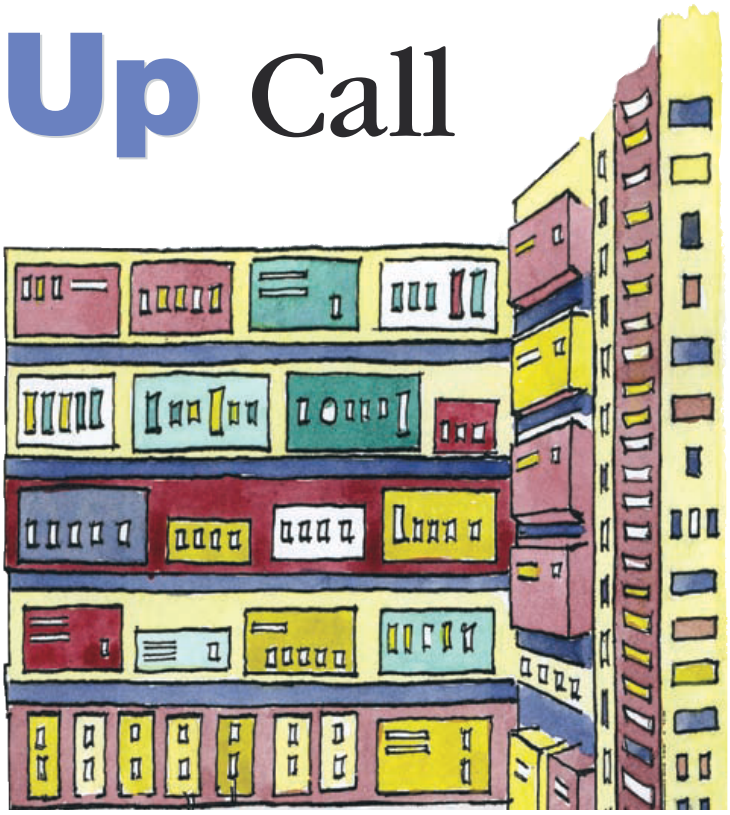
The 2006 Advisory Committee Notes (Notes) to that Rule further explain that the responding party must "identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing." The burden is on the non-producing party to support its position on a motion to compel or for a protective order.

Furthermore, if a party deletes arguably "inaccessible" ESI, the Notes to Rule 37(f) state that in determining whether to impose sanctions, one factor to be considered is "whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources."

How can a business satisfy this Rule, and stop any automated purge or other systems from operating on its "inaccessible" systems, until it has actually "accessed" its "inaccessible" systems, determined what automated programs are operational on those systems, and determined whether they might contain responsive ESI that is not also located on its "reasonably accessible" systems? Yet successfully doing so may undermine the non-producing party's claim that the ESI is inaccessible.

Jason Pickholz *is a shareholder in the New York office of Akerman Senterfitt.* **Stephanie Giammarco,** *a director with the litigation and fraud investigation practice at BDO Seidman, LLP, based in New York, leads the computer forensics and e-discovery practice areas.*

Are a Wake-Up Call



If the corporation waits to examine its policies and systems, counsel may be forced to recommend a prophylactic override of its automatic clean-up programs, and a system-wide rather than focused "litigation hold," which could cause a spike in retention costs while the business figures out its systems and what components might contain arguably responsive ESI. These costs and disruptions might be material for a smaller corporation; more so for a larger one with more expansive systems.

The Notes to Rule 26(f) acknowledge that the ordinary operation of computers involves the automatic deletion or overwriting of certain data, and that the "[c]omplete or broad cessation of a party's routine computer operations could paralyze the party's activities." And Rule 37(f) states that discovery sanctions may not be imposed on a party for failing to produce ESI as a result of the "routine, good-faith operation" of an ESI system absent exceptional circumstances.

The Notes to Rule 37(f) define "routine operation" as "the ways in which such systems are generally designed, programmed and implemented to meet the party's technical and business needs." However, those Notes also state that "good faith…may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation" such as pending or anticipated litigation, which may also qualify as "exceptional circumstances" under Rule 37(f).

One ambiguity that will need to be resolved is the definition of an "automatic" deletion system under Rules 26(f) and 37(f). Some "automatic" systems may allow or require the corporation to make judgments as to what the system will be programmed to "automatically" delete or overwrite. This in turn implicates the questions of what constitutes "routine operation" and what are legitimate "technical and business needs" relative to an automatic purging system, and whether that legitimacy is to be judged as of the time of implementation or in hindsight.

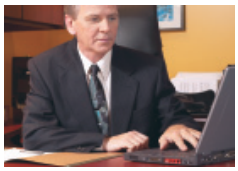
Continued on page S14

NEW YORK STATE BAR ASSOCIATION

GET A JOB.

(OR SOMEONE TO FILL IT.)

Sign up today at *www.nysba.org/lawjobs*



Find both through the New York State Bar Association. Our new partnership with American Lawyer Media's lawjobs.com website connects attorneys seeking new jobs with the firms that have them. Thousands of up-to-date job openings – and more than 50,000 qualified resumes in one place.

Together with career advice, a resume/cover letter builder, e-mail job alerts, salary information and the most streamlined search anywhere. All from the legal market's complete career solution.

NYSBA Member Benefit

Sign up today at *www.nysba.org/lawjobs*

NYSBA

ESI and the New Federal Rules

Continued from page S9

Related to "reasonably inaccessible" data is hidden "metadata" embedded in files. Metadata is not mentioned in the Rules but is alluded to in the Notes to Rule 26(f).

Some argue that metadata should be produced, like folder labels or other tags on paper documents, while others have noted that metadata is inherently unreliable and typically irrelevant.[3] For example, during a data migration, some systems record the creation date as the date of migration, and the creator as the person who migrated the data rather than its original author. How the courts will apply the new Rules to metadata remains to be seen.

Perils of Multiple Lawsuits

Where a corporation faces simultaneous lawsuits, because counsel handling each litigation will have to make the required representations during their respective Rule 26(f) conferences, the business must ensure that it accurately educates each of them with regard to its ESI systems and policies. Even a diligent company runs the risk that some information may be inadvertently omitted, or will be conveyed differently, or will be represented by each of its litigation counsel differently.

This creates a risk that counsel handling litigation "A" may represent during a Rule 26(f) conference, or may produce evidence during discovery on the corporation's "inaccessibility" claim, that certain ESI is inaccessible, while counsel in a second action "B" may concede that ESI relevant to that action residing on the same system is reasonably accessible. Alternatively, their respective descriptions of the corporation's automated systems, or its "routine operations" and "technical and business needs," may diverge.

Under either scenario, not only could the corporation face potential sanctions in litigation A,[4] but its counsel in that action could potentially be deemed in violation of his own obligations under Rule 26(f) and *Zubulake*. The adverse party in litigation A may cite the representations made or evidence produced in the other action to show that the company is playing discovery games or to support a spoliation claim. Potential adverse parties might rush to file their complaints and demand their Rule 26(f) conferences to force the corporation to capitulate to their settlement demands or risk facing motions for sanctions based on the alleged res judicata effect of the rulings in litigation A, as supported by the admissions in litigation B.

The business may now find its hands tied. If it adopts the position from litigation A that the ESI is inaccessible, these new parties will cite the adverse/sanctions rulings from litigation A and the admissions in litigation B. If it adopts the position from litigation B, that will undermine its ability to seek reconsideration of or to appeal the adverse/sanctions ruling in litigation A.

Conflicts With Foreign Laws

There are additional implications for multinational corporations.

A domestic company may be found to have enough influence with its foreign affiliates to require it to produce information stored abroad or face an adverse ruling in the domestic action. A foreign business may be required to produce its information under the theory that this is a "reasonably foreseeable cost of doing business" in the United States.

But because ESI may be reasonably accessible in the United States does not necessarily mean that same information is "reasonably accessible" in another country. Moreover, many nations and the European Union have their own privacy laws that might preclude disclosure of certain ESI.

For example, a recent internal investigation involved an Israeli firm with "secure data," i.e., documents generated by the company contained government-protected data that could be viewed only by employees with a certain level of government security clearance. Although counsel for the special litigation committee of the U.S. operation wanted to review the data sent to and from the company's Israeli employees, the Israeli operation insisted that counsel address the security issue first.

It was suggested that either only Israeli individuals with security clearance review the data, or that the secure portions of documents be redacted and all metadata embedded in those documents be "scrubbed." Thus, although similar documents were easily and readily accessible in the United States, several additional measures had to be implemented in Israel to prevent disclosure and transmission of protected ESI.

Under such circumstances, a domestic corporation may argue that although its foreign ESI is "reasonably accessible," it is unwilling to face foreign liability for producing it. The company may expose itself thereby to potential sanctions domestically and to piggyback suits seeking to capitalize on that representation. Inversely, if the domestic business argues that foreign laws render the ESI de facto "reasonably inaccessible," a court might disagree and find that the company has merely made a choice, in which case it might still be exposed to potential sanctions.

The new rules are visionary and long overdue. Nevertheless, waiting to react to them until the early stages of litigation is a potentially massive job that could disrupt a corporation's routine operations.

A Proactive Approach to ESI

The new Rules are visionary and long overdue. Nevertheless, reacting to them in the early stages of litigation is a potentially massive job that could disrupt a corporation's routine operations.

This assumes that the company already has formal policies and procedures in place, which is not necessarily the case even among exemplary organizations, given the constantly evolving state of technology and ever-mounting volume of ESI that require system upgrades or overhauls every few years, and that tax a business' storage capacity, budget and human resources at an ever-increasing rate.

One approach that might be taken now to ameliorate the burden of compliance with the new Federal Rules would be to form a proactive "ESI Team." That team should consist at a minimum of these two positions:

- an individual in the company's General Counsel's (GC) office—presumably a lawyer—who would be the liaison with the Information Technology (IT) department, interacting with that department and reporting back to the GC's office on what is going on in IT (the "IT Liaison"); and
- a counterpart in the organization's IT department whose job it is to work with the GC's office and the GC's representative on the ESI team (the "GC Liaison").[5]

The GC Liaison should work with the ESI Team to proactively accumulate and ensure the preservation and continuity of institutional knowledge, conduct an independent evaluation of the corporation's existing and legacy ESI systems and procedures; provide the GC's office and IT Liaison with input into the integration of new systems as they occur, and help to smooth ESI retention and retrieval should litigation arise.

Furthermore, the GC Liaison can assist during Rule 26(f) conferences with adverse parties. The GC Liaison can help supervise ESI searches and assist with implementing and monitoring compliance with litigation holds during discovery.

In addition, on a motion to compel ESI or for a protective order, the Notes to Rule 26(f) contemplate "taking depositions of witnesses knowledgeable about the responding party's information systems." The GC Liaison could serve as the corporation's witness, which might also lessen concerns that multiple designees in different litigations might provide inconsistent or inaccurate testimony.

The IT Liaison from the GC's office should work with the ESI Team and the GC's office to create or revise the corporation's ESI policies and procedures to comply with the new Rules, and implement roll-outs and other communications of those policies and procedures to employees. In addition, the IT Liaison should communicate those policies and procedures to the corporation's various litigation counsel, help litigation counsel fulfill their obligations under Rule 26 and *Zubulake* by keeping them informed of upgrades or modifications on an ongoing, real-time basis, coordinate and monitor along with the ESI Team the various litigation holds, and monitor the accuracy and consistency of the information conveyed across all litigations.

For multi-national corporations, the IT Liaison should work with foreign counsel to ascertain gaps between domestic and foreign discovery and privacy laws, analyze the corporation's legal options domestically and abroad, and formulate a cross-border discovery platform that will be ready to respond within the time frame required by Rule 26(f) should the need arise.

Despite the above, an IT department's main function is to support the business units; it is grossly inefficient, disruptive and expensive for it to suddenly suspend those functions for significant periods of time, repeatedly, in deference to litigation support. In addition, IT personnel may depart the corporation, resulting in a loss of institutional knowledge and increased costs attributable to training the new personnel about litigation support.

Similarly, the GC's office must be available to deal with a variety of legal, business, compliance and other issues facing the corporation daily. The enormity of the obligations imposed by the new Rules could eventually consume a GC's office, to the detriment of those other functions.

One solution is to add an independent ESI consultant and an outside ESI counsel to the ESI Team. Not only would this free up internal corporate staff and officers to focus on business issues, but, in conjunction with the ESI Team and the GC, an independent ESI consultant may have more credibility than a corporate employee at the Rule 26(f) conference or as the corporation's witness.

In addition, outside ESI Counsel with a litigation background and familiarity with the new Rules could provide a significant coordinating link for ESI purposes between the corporation, its various litigation counsel and if applicable its foreign affiliates and foreign counsel and help ensure consistency across the board of the dissemination of its ESI-related systems information and its legal positions with regard thereto.

The amendments to the Rules are as much a call to all parties to get their ESI houses in order as they are procedural rules. By taking a proactive approach to ESI, and institutionalizing it as a component of business operations, corporations can go a long way toward anticipating ESI-related litigation costs, spreading those costs out over time, focusing ESI discovery procedures, streamlining internal forensics investigations and taking much of the ambiguity and sting out of their new obligations under the Rules.

1. To calculate timing, Rule 26(f) should be read in conjunction with Rule 16(b).

2. *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("*Zubulake V*").

3. See, e.g., THE SEDONA PRINCIPLES: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT DISCOVERY, pp. 5-6, Principle 12, Cmt. 12.a. (The Sedona Conference Working Group Series, July 2005 Version) (noting "the real danger" that metadata "may be inaccurate").

4. See, e.g., *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, Case No. 502003 (15th Jud. Cir. Fla. 2005) (entering default judgment as sanction, ordering that liability allegations of complaint be read to jury and deemed established for all purposes).

5. It may also be advisable for liaisons from business units to inform the ESI Team with regard to how the particular unit utilizes ESI systems and what its procedures are in practice.