The New Federal Rules of Civil Procedure: What Every Corporate Counsel Should Know and Do

By N. Thomas Connally and Jon M. Talotta.∗

Litigation officially enters the information age on December 1, 2006, when amendments to the Federal Rules of Civil Procedure go into effect expressly aimed at discovery of electronically stored information ("ESI"). The new rules are intended to address three broadly-defined aspects of electronic discovery ("e-discovery"): (1) issue identification, (2) production, and (3) preservation.

Corporate counsel should view these changes as a clarion call to revisit (or finally develop) ESI policies and prepare in advance of litigation to handle e-discovery issues. Doing so will allow you to better manage e-discovery costs, protect your business information, and reduce the risk of spoliation claims.

Three Key Aspects of E-Discovery Affected

1. Issue Identification. Changes to Rules 16 and 26 require parties to identify potential e-discovery issues at the outset of litigation:

- Pre-Discovery Conferences, Rule 26(f). Parties must discuss issues relating to ESI preservation and production, including the form(s) in which ESI will be produced, issues relating to privileged and protected information, and inadvertent disclosures.

- Scheduling Orders, Rule 16(b). Scheduling orders must address disclosure and discovery of ESI, and any agreements between the parties for dealing with privileged and protected information, including inadvertent disclosures.

- Initial Disclosures, Rule 26(a). Initial disclosures must identify and describe sources of ESI.

These new rules place a premium on knowledge and preparation. To that end, review your company's ESI policy. If you do not have one, develop one. Get to know

---

∗ Tom is a litigation partner and Jon is a senior litigation associate in Hogan & Hartson LLP's Northern Virginia office. In addition to focusing their practices on complex litigation, they regularly advise clients, publish and speak on issues relating to electronically stored information, electronic discovery and records management practices.

your company's ESI systems. Breadth of knowledge is more important than depth – you cannot know all the answers regarding your company's systems and ESI, but you need to know what questions to ask and who will have the answers. Thus, get to know the key records and IT personnel who manage and know your systems, and educate them on their role in e-discovery. If you do not have a working understanding of your company's systems and ESI, or you fail to educate your key records and IT personnel about how e-discovery now works, your company will stumble out of the blocks and find itself playing catch-up throughout each new federal case in which it is a party.

2. Production. Changes to Rules 26, 33 and 34 provide protections to requesting and producing parties, and establish a framework for resolving e-discovery disputes, including potential cost-shifting:

- Inaccessible ESI, Rule 26(b)(2). Producing parties can seek protection from producing responsive ESI based on undue burden or cost. Initially, responsive ESI that is unreasonably burdensome or expensive to produce (e.g., located only on disaster recovery tapes, isolated on inactive legacy systems) may be identified but not produced. The requesting party may then petition the court to compel production. Courts are empowered to enter a protective order, order production, or shift the costs of retrieval and production onto the requesting party (although the producing party still will bear the costs of review).

- Form of ESI Productions, Rule 34(b). Requesting parties now can specify the form(s) in which ESI is to be produced (e.g., native files, exported files, PDFs, TIFFs), so that they can make fair and efficient use of the information. Producing parties can object to the requested form because, depending on the circumstances of a particular case, each of the various forms of production can present problems (e.g., inability to redact, risk of alteration, limited searchability). In resolving disputes, courts are likely to find guidance in Rule 34(b)(ii), which states that if a particular form for production is not specified by the requesting party, the producing party shall produce its ESI in the form in which it is usually maintained, or in a form that is reasonably usable. These same concepts have been adopted for subpoenas to non-parties (see Rule 45).

- Other Noteworthy Changes, Rules 33(d) and 34. A responding party may now produce ESI (like the ability to produce hard copy documents in the past) in lieu of answering an interrogatory (see Rule 33(d)), and a requesting party may now request to inspect, test, or sample designated ESI (see Rule 34).

These changes are intended to bring much needed order, consistency and baseline rules of reason to e-discovery, as well as to limit gamesmanship and the use of e-discovery as a weapon in litigation. Parties that make sweeping requests now face the risk that they will end up paying for at least part of the requested production. Producing ESI in the least usable form (perhaps in order to limit an opposing party's ability to search, organize and use the information) is no longer an advisable option.

Companies also need to be prepared to invest in systems and technology – either on their own, or through their outside counsel or vendors – to effectively and efficiently manage the identification, review and production of their own ESI, as well as the review and analysis of ESI produced by other parties.

3. Preservation. Changes to Rules 26 and 37 provide protections against the ever-present risks of inadvertent disclosures of privileged or protected information, and claims of spoliation:

- Inadvertent Disclosures, Rule 26(b)(5). All ESI productions, particularly large ones, carry the risk of inadvertent disclosures. Attempting to resolve the discord among federal circuits on how inadvertent disclosures are to be handled, the new rules allow a producing party to notify a receiving party of an inadvertent disclosure and the basis for the assertion of privilege or other protection. Upon notification, the receiving party must "promptly return, sequester, or destroy" the information and "may not use or disclose" it until the claim is resolved by agreement or the court. The same concepts have been adopted for subpoenas to non-parties (see Rule 45).

- "Quick Peek" and "Claw Back" Provisions, Rules 16(b) and 26(f). Among the agreements parties are encouraged to negotiate at the outset of litigation are so-called "quick peek" and "claw back" arrangements, enabling the producing party to make certain ESI available for a preliminary review by the requesting party, subject to later assertions of privilege or other protection once the requesting party has selected specific records for production.

- Spoliation Safe Harbor, Rule 37(f). Recognizing the reality that all ESI cannot and need not be saved, and in order to reduce the proliferation of spoliation claims alleging intentional/negligent destruction, the new rules now provide a safe harbor for the routine deletion of ESI. "Absent exceptional circumstances," courts may not sanction a party for deleting or erasing ESI "as a result of the routine, good-faith operation" of its ESI systems.

Again, knowledge and preparation are key. These protections will have little or no value to your company if it has unsound ESI policies (or none at all) and its legal, records and IT personnel are not well coordinated. For example, if a company cannot explain coherently and comprehensively what ESI it saves and why, generally, it will be hard-pressed to justify deletion or erasure of the specific ESI at issue in a spoliation claim. As a result, there is no question that investing in ESI best practices will lower a company's exposure to litigation expense and liability.

Act Now, Plan Ahead

This brief summary should make one thing clear – businesses need to prepare in advance of litigation in order to handle e-discovery efficiently and effectively. Sound ESI policies are essential, including provisions for holds on the destruction of potentially relevant ESI during litigation. Records and IT personnel who oversee and operate your

company's systems need to understand their role in e-discovery before the curtain rises and they need to perform in a deposition, discovery hearing, or trial. The favorable resolution of discovery disputes or the admissibility of critical evidence may turn on your IT representative's ability to explain your company's systems and defend its practices in layman's terms.

Many forward-thinking corporate counsel, particularly at large companies that are regularly involved in litigation, recognized some time ago the potential benefits of sound ESI policies and proactive litigation strategies. Some already have begun taking the next steps in litigation preparedness – conducting audit-like reviews of their ESI policies, developing standard templates and routine procedures for the identification, disclosure, production and management of ESI, and investing in technology to aid and automate these processes. Such preparation provides reward in at least three ways:

- Avoiding Conflicting Positions and Mistakes. If it has a standard approach and disclosure templates, a company reduces the risk that it will (a) make conflicting disclosures and assertions regarding its ESI and records management across different cases, or (b) mismanage or destroy discoverable ESI, with potentially disastrous results.

- Reducing Burden of Litigation on Employees. By moving away from an ad hoc approach, a company can streamline the process of identifying, gathering, reviewing and producing ESI, greatly reducing the burden of each new case on legal, records, IT, operations and management personnel.

- Lowering Expense and Exposure. Standard processes and thoughtful automation promote efficiency and effectiveness in e-discovery, reducing both cost and risk.

The amendments are designed to limit the potentially crushing burden of e-discovery on parties in federal litigation, but the new rules do not operate on their own to make e-discovery easier and less expensive – they merely provide tools parties can use to reduce their own burden and expense, as well as to conduct more efficient and effective e-discovery on other parties. Only those companies that are proactive, knowledgeable and prepared to handle e-discovery will be able to pick up these tools and use them immediately. Those companies that fail to act will soon find these tools being used effectively against them.