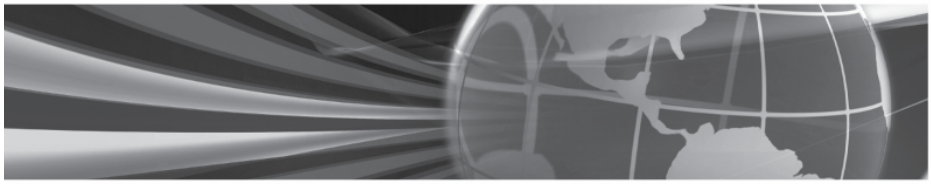
Greenberg Traurig

ALERT: eDiscovery & eRetention



September 2006

The Impact of the New Federal Rules of Civil Procedure on Electronic Discovery

On December 1, 2006, new amendments to the federal rules of civil procedure governing electronic discovery are scheduled to become effective. For those who have been following developments concerning electronic discovery the last few years, the new rules will be a consolidation, clarification and extension of developing law. For those who haven't, the new rules will be a stunning revelation of the impact of technology upon litigation.

These amendments are the most important changes in the discovery rules since at least 1970, and perhaps since the current civil discovery structure was created in 1938. The changes will not only impact the discovery and trial of civil cases, but also will sail upstream to shape the creation, management and retention of electronically stored information. Judges, litigators and litigation support teams must, of course, understand these amendments, but so must executives, information technologists, records managers, risk managers and financial officers.

This alert summarizes the likely impact of these new federal rules. The advisory committee notes ("Notes") that accompany and explain the new rules are rich and detailed, and answer some questions raised. This alert relies on both the rules and the Notes. All quoted language below is from the rules or Notes.

Electronically Stored Information

Electronically stored information is now the dominant method of storing human information. Over 99% of new information stored in the United States is stored electronically. See generally David K. Isom, Electronic Discovery Primer for Judges, http://fclr.org/2005fedctslrev1.htm. The rules add "electronically stored information" (ESI) to "documents" and "things" that may be inspected or produced under the rules. The advisory committee ("Committee") debated whether "document" was an adequate label for the breadth of discoverable data, especially since "document" had been interpreted broadly since 1970 to include all types of electronic data. The Committee decided to add ESI because it concluded that many evolving types of digital data, especially dynamic data, are difficult to characterize as "documents." The Committee concluded that the rules should address significant issues presented by ESI not presented by paper discovery, including the fact that ESI "is retained in exponentially great

volume," "is dynamic," and "may be incomprehensible when separated from the system that created it."

Economic Pragmatism

The new rules emphasize that controversies over the scope of discovery often will be resolved by balancing the burdens of providing the discovery against the potential benefit of the discovery. Questions such as whether certain data is inaccessible, whether certain deleted data is discoverable, and whether certain production formats are acceptable, will likely be resolved by balancing these rules-based factors:

(1) whether the ESI is unreasonably duplicative or cumulative;

(2) whether the ESI can be obtained from a less burdensome source;

(3) whether the seeking party has had ample opportunity to obtain the ESI;

(4) the needs of the case;

(5) the amount in controversy;

(6) the parties' resources;

(7) the importance of the issues in the litigation;

(8) the importance of the ESI in resolving the dispute.

Destruction of ESI and the "Safe Harbor" from Sanctions

The new rules provide "limited protection" against sanctions for a party's inability to provide its relevant ESI lost as a result of the good-faith "routine modification, overwriting and deletion of information that attends normal use." During the development of the new rules, this provision was known as a "safe harbor," but this label disappeared from the final draft because this rule now offers little protection from sanctions for destruction of relevant ESI:

- ***Good Faith***

  No protection from sanctions under the rules exists if "parties … intentionally destroy information because of its relationship to litigation." The rules have "adopted essentially a negligence test, requiring that the party seeking protection has taken reasonable steps to preserve information after it knew the information was discoverable in the action." The Notes equate this requirement with the steps often called a "litigation hold," discussed below.

Factors that will bear on whether the information loss is protected from sanctions under the rules include: (1) whether the conduct violated a court order or discovery stipulation among the parties; (2) what steps the party took to determine whether it was feasible to intervene to modify or suspend routine systemic destruction of information.

- ***Routine Operation***

The loss of information must have resulted from routine computer operations, including routine data loss through operations "designed, programmed and implemented to meet the party's technical and business needs," including the "alteration and overwriting of information, often without the operator's specific direction or awareness."

- ***Rules-Based Sanctions***

Even if a party can establish that the loss of its ESI was unintentional and despite good faith efforts to preserve relevant evidence, the rules only prevent "sanctions under these rules." A party can still receive penalties for preservation spoliation or retention spoliation (discussed below) based on the inherent authority of the Court to sanction parties or based on violations of other statutory, regulatory or ethical requirements.

Document Retention

The Notes clarify that the new rules do not diminish a company's statutory or regulatory duty to retain documents or ESI. Indeed, as discussed below, the new rules increase the probability that relevant inaccessible data will at least need to be identified, and possibly produced. Companies should therefore give renewed attention to retaining their documents and ESI in compliance with their statutory and regulatory obligations, and furthermore, to retaining their documents and ESI so that they can be accessed efficiently and cost-effectively in litigation.

Preservation and Litigation Holds

The Committee considered creating or defining a preservation duty in the federal rules of civil procedure, but decided to leave the duty where it already existed -- in the common law (primarily state tort law), criminal law, and ethical rules. The rules explicitly do "not undermine or reduce common law or statutory preservation obligations."

On the other hand, the Notes repeatedly endorse a thoughtful, workable litigation hold process to preserve ESI for litigation. The Notes, for example, recognize that the diligence concerning the litigation hold process may impact a decision whether a party was acting in good faith in connection with the loss of relevant data, and direct that the

preservation duty and process be discussed in the early attorney and court-directed discovery conferences.

Production and Direct Inspection

Like the current rules, the new rules will allow two types of document requests: a request that the other party "produce" documents, and a request that the requesting party be allowed direct access to "inspect" documents. By adding ESI to the direct access rule, the new rules clearly allow under some circumstances that a party may be entitled to direct access to inspect an opponent's information systems. The Committee recognized, however, that direct access "creates risks of privilege invasion, business interruption, data destruction, and exposure of irrelevant data, among other risks."

Destruction versus Deletion

The new rules recognize several functional distinctions between ESI and paper documents. One of these distinctions is that, unlike paper, electronic media have an entire spectrum of methods for getting rid of or reducing access to information. One end of the spectrum is "deletion," which generally makes data somewhat less accessible and less apparent to a computer user, but is generally recoverable. The other end of the spectrum, "destruction," makes information absolutely, physically unrecoverable, such as by grinding and melting. Between these ends of the spectrum are processes variously called, on various media, overwriting, recycling, degaussing, disposal, sanitizing, clearing or purging, and these methods may leave data more or less accessible and more or less burdensome to recover.

Most recent cases hold that the mere deletion of information does not place that information beyond discovery in civil litigation. If the deletion, however, affects such issues as accessibility, production costs, and whether the loss of or failure to produce information was in good faith, for example, deletion may impact discoverability and the Court's determination as to which party should bear (or share) the cost of collecting and providing the information: "Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as 'embedded data' or 'embedded edits') in an electronic file but not make them apparent to the reader…. Whether this information should be produced may be among the topics discussed in the Rule 26(f) conference."

The Notes provide that deletion may make data "inaccessible." "Examples [of inaccessible data] from current technology include … data that was 'deleted' but remains in fragmented form, requiring a modern version of forensics to restore and retrieve…." However, as described below, under the new rules the fact that data is "inaccessible" does not mean the parties do not need to address the treatment of that data in the litigation.

Early Electronic Discovery Readiness

Under the new rules, parties will need to understand their electronic data early in the litigation. In addition to needing to make initial disclosures (discussed below), parties will need to attend a "prediscovery conference" and negotiate electronic discovery issues within weeks of service of the summons and complaint, if the case involves electronic discovery. Parties will need to be prepared to stipulate, if possible, and discuss with the court, typically within weeks of service, a proposed discovery plan and schedule that includes the treatment of ESI.

The rules and Notes include the following among electronic discovery issues be addressed or considered in order to develop this discovery plan early in the litigation for cases involving electronic discovery:

(1) what data is inaccessible;

(2) the scope of the ESI to be preserved or discovered;

(3) the existence of a "litigation hold";

(4) the format of preservation and production of ESI;

(5) whether, to what extent, and how to prevent the routine destruction of potentially discoverable information;

(6) the scope of privilege and work product protection, the process for asserting such privileges and protections, and possible methods for doing privilege reviews cost-effectively without waiving the privilege between the parties;

(7) the timing, form and requirement for initial disclosures of ESI;

(8) the timing of discovery;

(9) whether discovery should be conducted in phases or a certain sequence;

(10) the sources of information to be searched.

Initial Disclosures

Under the current rules, early in civil litigation, without awaiting a discovery request from an opponent, a party must produce to the opponent documents that the disclosing party may use to support its claims or defenses. The new rules specify that supporting ESI must also be included in these initial disclosures. The new rules also direct that these initial disclosures, including the format of these disclosures, must be considered in the early attorney and court conferences. The Committee recognized that the ESI that must

be disclosed early in the litigation is "often voluminous and dispersed, [and] can be burdensome to locate and review," but concluded the initial disclosure rules apply to ESI.

Depositions of Corporate Representatives

Depositions of corporate information managers and technologists are an effective way to assess an adversary's information systems, technology and ESI. The Notes recognize the utility of these depositions taken pursuant to Rule 30(b)(6). For example, it may be useful in resolving disputes about what data is inaccessible to take "depositions of witnesses knowledgeable about the responding party's information systems."

Privilege

In general, documents protected by the attorney-client privilege or attorney work product doctrine become unprotected if the documents are produced to an opponent. The Committee recognized that the cost of privilege review for ESI can far exceed the cost of privilege review for paper documents: "reviewing ESI for privilege and work product protection adds to the expense and delay, and risk of waiver, because of the added volume, the dynamic nature of the information, and the complexities of locating potentially privileged information."

The new rules require that, early in the litigation, the parties should discuss, and the court should consider, "issues relating to claims of privilege or of protection as trial-preparation material, including if the parties agree on a procedure to assert such claims after production whether to ask the court to include their agreement in an order." The court can enter an order approving the parties' agreement regarding a process for reviewing and producing documents without waiving privilege or work product protection. Two types of agreements are mentioned as possible examples: (1) a "quick peek" agreement that the requesting party can examine documents or systems briefly without waiving privilege as to any document reviewed on the hope that the volume of documents can be reduced before a serious privilege review is done; (2) a "clawback" agreement that production of a privileged document to an adversary will not waive privilege so long as the producing party asserts privilege within a short time after the party realizes that a produced document should have been withheld as privileged.

The utility of these "non-waiver" agreements appears limited.

First, the production of privileged information pursuant to a non-waiver agreement in a federal case, even if court-approved, may not be recognized as preventing a waiver of privilege under state law.

Second, even if a "non-waiver" agreement is treated as effective between the agreeing parties, the rules provide no assurances that third parties to a court-ordered "non-waiver" agreement will be unable to effectively claim that the once-privileged ESI is

privileged no more based on the prior disclosure to an adverse party pursuant to a "non-waiver" agreement.

Accordingly, there are good reasons not to rely on a "quick peek", "clawback" or other "non-waiver" agreement as a short-term solution to reducing the burden of a privilege review of ESI before fully considering the risks of waiver in other litigation. This is especially so if a party believes that the same ESI is likely to be at issue in litigation with third parties to the "non-waiver" agreement.

Inaccessible Data

One of the few rule amendments expressly designed to change current practice is the provision applicable to inaccessible data. Touted as "an improvement over the present practice, in which parties simply do not produce inaccessible ESI," the new rule both demands that the parties not ignore or forget relevant inaccessible data, and also provides a buffer against the need to produce some inaccessible data.

Under the new rules, a party initially will not need to "provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." This new rule "requires the responding party to identify the sources of information that were not searched, clarifying and focusing the issue for the requesting party." If the seeking party, normally after reviewing the produced accessible ESI, moves to compel discovery of information from sources identified as inaccessible, the requested party must prove that the information is not reasonably accessible. "If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows goods cause," considering the factors to be balanced that are listed in paragraph 2 above.

The following is a recommended approach for dealing with inaccessible data under the new federal rules:

(1) Preserve inaccessible data. Since the rules allow the seeking party to challenge a party's decision not to produce inaccessible data, it is clear that inaccessible data must be preserved. "A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence." If the very process of preserving inaccessible data is unduly burdensome, however, the responding party should seek a protective order from the court restricting the preservation duty. "Among the reasons that may lead a responding party to raise the issue is to resolve whether, or the extent to which, it must preserve the information stored on the difficult-to-access sources until discoverability is resolved."

(2) Produce accessible data first. "Lawyers sophisticated in these problems are developing a two-tier practice in which they first sort through the information that can be provided from easily accessed sources and then determine whether it is necessary to search the difficult-to-access sources."

(3) Identify sources of inaccessible data. This new rule provides protections for parties that identify to an adversary inaccessible ESI early in the litigation. Therefore, a party should sufficiently assess its data sources so that early in the litigation it is able to identify its inaccessible ESI. This identification need not be exhaustive: only "sources", not individual documents, need be identified, and sources need only be identified "by category or type." However, the "identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources."

Production Format

The new rules distinguish storage format from production format. Provisions relating to storage format are deliberately broad and flexible. The Notes make clear, for example, that a request for "documents" is to be deemed to include both paper documents and ESI.

Production format is different.

Under the new rules, it will be important for the requesting party to specify in document requests and subpoenas the desired production format. The Committee recognized that production format was not usually a major issue with paper, but has become a major issue with ESI. The requesting party will now be able to specify the form or forms of production. This right should always be exercised thoughtfully, since a failure to do so will convey to the producing party the right to decide which "default format" to use -- either the form in which the information is ordinarily kept or "a form or forms that are reasonably usable," even if that form is not ordinarily used by the producing party. (This, however, "does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in litigation.") The requesting party must also bear in mind when specifying a format for the production of ESI that an adversary will often respond by seeking the same ESI production format from the requesting party.

A specifically requested production format, on the other hand, must be honored by the responding party unless the responding party moves for protection and shows that the requested format would be unduly burdensome.

The producing party need produce only one copy of duplicate documents, and only in one format.

Subpoenas

The new rules make the process of subpoenaing ESI similar to the process of requesting ESI from a party. For example, the rules relating to privilege, inaccessibility, production format, and safe harbor protection against the good-faith, routine loss of computer information, are the same for subpoenas as for document requests. As before, Rule 45 continues to protect non-parties from costs and burdens that parties normally must bear.

Metadata

ESI almost always includes more data than is apparent when the document is viewed on a screen or printed to paper. This additional data is metadata. Metadata may include system files or other data of which the user may is not aware that is necessary to the operation of the computer. The Notes refer to metadata as "automatically created identifying information about the history or management of an electronic file" and "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 is clearly discoverable under the new rules. The sole fact that data is classified as metadata does not change its discoverability. In a particular instance, however, metadata might be irrelevant, or inaccessible, or inadvertently destroyed, or privileged, and these factors might affect the discoverability and admissibility of metadata. The Notes recognize, for example, that understanding what metadata may be privileged is a "complexity" that argues in favor of allowing production of metadata under some circumstances without waiving privilege. The risks of forfeiting privilege or protection as to metadata are similar to the risks inherent in producing other data to an adversary.

Typically, variations in metadata are what make different production formats functionally disparate. Metadata is therefore a key factor in negotiations concerning production formats.

This Alert was written by David K. Isom, co-chair of the eDiscovery & eRetention Practice Group and Philip H. Cohen, a member of the eDiscovery & eRetention Practice Group. If you have any questions regarding the subject matter of this GT Alert, please contact Mr. Isom at 303.685.7404, Mr. Cohen at 212.801.2145 or your Greenberg Traurig liaison

Albany
518.689.1400

Amsterdam
+ 31 20 301 7300

Atlanta
678.553.2100

Boca Raton
561.955.7600

Boston
617.310.6000

Chicago
312.456.8400

Dallas
972.419.1250

Delaware
302.661.7000

Denver
303.572.6500

Fort Lauderdale
954.765.0500

Houston
713.374.3500

Las Vegas
702.792.3773

Los Angeles
310.586.7700

Miami
305.579.0500

New Jersey
973.360.7900

New York
212.801.9200

Orange County
714.708.6500

Orlando
407.420.1000

Philadelphia
215.988.7800

Phoenix
602.445.8000

Sacramento
916.442.1111

Silicon Valley
650.328.8500

Tallahassee
850.222.6891

Tampa
813.318.5700

Tokyo
+ 81 3 3264 0671

Tysons Corner
703.749.1300

Washington, D.C.
202.331.3100

West Palm Beach
561.650.7900

Zurich
+ 41 1 364 26 00