Paul Hastings

November 2006

StayCurrent

A Client Alert from Paul Hastings

New E-Discovery Rules: Is Your Company Prepared?

By Maureen O'Neill, Kirby Behre and Anne Nergaard

On December 1, 2006, amendments to the Federal Rules of Civil Procedure ("FRCP") concerning the discovery of electronically stored information go into effect. These so-called "e-discovery rules" are noteworthy for several reasons. First, the implementation of these rules marks the first time the FRCP have expressly addressed electronically stored information ("ESI") and the obligations of parties to address e-discovery issues. Parties are now required to provide their adversaries early in the litigation with precise information about the sources of relevant ESI and to discuss how such information will be handled over the course of the litigation. Second, the commentary to the new e-discovery rules broadly defines ESI to include not only e-mails, word processing documents, and databases, but "any type of information that is stored electronically." Third, the new rules expressly address a problem unique to ESI – that some sources of ESI are not "reasonably accessible" without significant cost or burden to the producing party. Finally, the rules recognize that the production of large volumes of electronic information increases the risk that the producing party will inadvertently produce privileged materials and provide a protocol for resolving claims of inadvertent disclosure. The overarching theme of the new e-discovery rules is one of full disclosure and discussion of e-discovery issues among the parties.

This Client Alert briefly describes the major provisions of the new e-discovery rules, and offers guidance for preparing your company for the new ways in which e-discovery issues must be handled in litigation.

WHAT TOPICS DO THE NEW RULES COVER?

The new e-discovery rules are found in amendments to FRCP 16, 26, 33, 34, 37 and 45. The topics addressed by these new rules include what constitutes ESI; the format in which ESI is produced; parties' obligations to disclose ESI; limits on discovery of not reasonably accessible ESI; the inadvertent production of privileged materials; and the consequences of the good faith loss or deletion of ESI.

What Constitutes ESI

ESI is not limited to the most common information produced in discovery such as e-mails, word processing documents, and databases. Rather, the Advisory Committee notes to Rule 34 advise that ESI should be defined expansively, and quite literally includes "any type of information that is stored electronically."

The Format In Which ESI Is To Be Produced

A requesting party may specify the format in which it wants ESI produced. *See* Rule 34(b). However, parties are encouraged to reach agreement about the format in which ESI will be produced in their early planning conference. *See* Rule 26(f)(3). If the parties are unable to reach such an agreement, and if the requesting party does not specify the format, Rule 34(b)(ii) instructs the responding party to produce ESI either in "a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable." Thus, a party may be required to convert its data to a format that other parties may use. To fulfill this obligation, parties may be required to provide information about the software necessary to access the data, or other reasonable technical support.

Obligations To Disclose ESI

Disclosure of ESI must be addressed at the onset of the lawsuit, as the parties' initial discovery plan must include a discussion of "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." Rule 26(f)(3); *see also* Form 35.

Next, each party must provide "a description by category and location of … electronically stored information … that the disclosing party may use to

support its claims or defenses" in their Rule 26(a)(1)(B) disclosures. The specific timing of the Rule 26(a) disclosures varies by jurisdiction, but they must be made early in the lawsuit, typically before the discovery period has opened. Parties must provide these disclosures without waiting for a request for such information. *See* Rule 26(a)(1).

Not only are parties required to identify what ESI they possess and will be producing, but they also must disclose what ESI they are *not* producing. Specifically, the new e-discovery rules require a party to identify, by category or type, any sources of ESI that are "not reasonably accessible" and that are not being searched or produced.

Limits On Discovery Of Not Reasonably Accessible ESI

Rule 26(b)(3)(B) places limits on the discovery of "electronically stored information from sources that the [responding] party identifies as not reasonably accessible because of undue burden or cost." The term "not reasonably accessible" is not defined in the FRCP, however, and certainly will be the subject of dispute in many cases. Whether ESI is reasonably accessible will depend on the cost and burden of producing the information, which typically will be driven by the extent to which such data must be restored, converted or otherwise manipulated electronically before it can be reviewed or analyzed.

The Advisory Committee notes provide that the responding party should provide enough detail about the purportedly not reasonably accessible ESI to allow the requesting party to decide whether to challenge the refusal to search or produce. Such a decision requires a fact-specific evaluation of the burdens and costs of providing the discovery and the likelihood of finding responsive information. *See* Rule 26(b)(2) Advisory Committee notes. Parties are encouraged to resolve disputes about the accessibility of ESI without court intervention by discussing such issues as the "burdens and costs of accessing and retrieving the information, the needs that may establish good cause for requiring all or part of the requested discovery even if the information sought is not reasonably accessible, and conditions on obtaining and producing the information that may be appropriate." Rule 26(b)(2) Advisory Committee notes.

If the requesting party ultimately moves to compel production of the information, the responding party bears the burden of justifying the "not reasonably accessible" designation by showing the "undue burden and cost." Even if that showing is made, the requesting party may nevertheless secure production of the information if it shows "good cause." The Advisory Committee notes set out seven non-exclusive factors to be considered in the assessment of good cause, including, for example, the specificity of the discovery request, the likelihood of finding relevant information that cannot be found in more easily accessible sources, the importance of the issues at stake in the litigation, and the parties' resources.

Importantly, identification of ESI as not reasonably accessible does not relieve a party of the obligation to preserve such information. *See* Rule 26(b)(2) Advisory Committee notes. Whether such an obligation exists depends on the facts of each case.

Inadvertent Disclosure Of Privileged Or Work Product Information

The potential for inadvertent production of privileged or work product materials, and the need to assert post-production claims of such protection, is heightened with the discovery of enormous volumes of electronically stored information. Rule 26(f) requires parties to discuss issues "relating to claims of privilege or 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." This new rule requires the parties to discuss and perhaps reach agreement regarding how claims of inadvertent disclosure of privileged or work product information will be addressed. Should the parties not reach such an agreement, Rule 26(b)(5)(B) sets forth some baseline procedural rules for handling post-production claims of privilege or work product.

The Advisory Committee notes make clear that these new provisions govern only the procedure for addressing inadvertently produced materials – they do not affect the substantive determination of whether such inadvertent production has waived the asserted privilege. Also, litigants should keep in mind that any agreements reached by the parties about the procedural or substantive handling of inadvertent production may not be enforceable as to third parties.

Good-Faith Loss Or Deletion Of ESI

Generally, parties may be sanctioned for failing to meet their obligations to preserve relevant ESI. Rule 37 provides an exception where the loss of ESI results from

a "routine, good faith" operation of an information system. This exception recognizes the unique nature of many sources of ESI, which are subject to automatic deletion or overwriting in the normal course of business.

With respect to "not reasonably accessible" ESI, whether "good faith" requires a party to take steps to prevent the loss of such information depends on the circumstances. One relevant factor is whether the "party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources." Rule 37(f) Advisory Committee note.

WHAT CAN YOU DO NOW TO PREPARE?

Take An ESI Inventory

The new e-discovery rules require parties to identify and disclose a significant amount of information about the ESI they maintain, and to engage in strategic negotiations with opposing counsel about the handling of ESI in litigation. Companies should gather that information now, even if no litigation is pending, to provide a significant advantage if and when litigation commences.

The legal department should have a thorough understanding of all types of ESI maintained by the company and its practices for managing this information. At a minimum, the preparation of an "ESI inventory" should include a review and inventory of data systems and storage – covering hardware and software – at both the corporate level and the individual custodian level.

With respect to each source of ESI identified, counsel should obtain information sufficient to develop a strategy for disclosing and potentially producing the information if litigation arises. A wide range of information may inform this strategy, including: (1) the time frame that the information was or is in use; (2) the substantive content of the information source; (3) the natural (or "native") format of the information; (4) the methods for accessing and retrieving the information; (5) the costs of retaining, accessing, and producing the information; (6) the current retention schedule; (7) the business justification for retaining the data; and (8) legal and regulatory mandates to retain the data.

Implement, Review, And Monitor Retention Policies

Companies should implement legally defensible, reasonable, good faith policies and procedures for the retention of documents and ESI. These policies and procedures should be reviewed on a regular basis to take into account new sources of data and types of technology. The Sedona Guidelines for Managing Information and Records in the Electronic Age provide five useful points of guidance on retention policies and procedures:

- An organization should have reasonable policies and procedures for managing its information and records.
- An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.
- An organization need not retain all electronic information ever generated or received.
- An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.
- An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

See The Sedona Guidelines: Best Practices Guidelines & Commentary for Managing Information & Records in The Electronic Age (September 2005), *available at* www.thesedonaconference.org.

It is critical that retention policies are monitored, audited, enforced, and modified as necessary. Specifically, a company should ensure that information technology ("IT") personnel are educated on retention policies, provide input on the feasibility of retention procedures, and understand the consequences of failing to follow such policies and procedures.

Develop A Litigation Response Protocol

Companies should develop a litigation response protocol for preserving relevant information – *i.e.*, implementing a "litigation hold" – which can be quickly and consistently applied when preservation obligations arise. A consistent litigation hold protocol will inform the negotiations now required at the early meeting of counsel about "any issues relating to preserving discoverable information."

A litigation response protocol also will help establish the good faith exception to sanctions under Rule 37(f).

A reasonable litigation response protocol should include the following elements:

- A template for litigation hold instructions, which may include a definition of all documents and data to be preserved, the procedure for retaining such documents and data, the method of distribution to and acknowledgement of receipt by employees, and the specified frequency for re-distribution of the litigation hold instruction;
- A required distribution list for all litigation hold instructions that includes IT and Human Resources professionals, and a protocol for identifying other appropriate custodians to include on particular litigation hold orders; and
- A plan for identifying potentially relevant sources of ESI and halting the regular retention schedule for this information.

CONCLUSION

Complying with the new e-discovery rules will almost inevitably place a burden on a company's time and resources in the near term. After this initial investment is made, however, in the long term a company will be able to develop a consistent and strategic approach to e-discovery, negotiate effectively about e-discovery, minimize the costs and burdens of e-discovery, meet its e-discovery obligations, and reduce the risk of sanctions for failing to produce ESI.

If you have any questions regarding the new e-discovery rules or other e-discovery issues, please contact any of the following members of our E-Discovery Group:

Atlanta

Maureen E. O'Neill
404-815-2219
maureenoneill@paulhastings.com

W. Cory Barker
404-815-2379
corybarker@paulhastings.com

R. Matthew Martin
404-815-2205
mattmartin@paulhastings.com

Los Angeles

Jason M. Frank
213-683-6146
jasonfrank@paulhastings.com

Heather A. Morgan
213- 683-6188
heathermorgan@paulhastings.com

New York

Richard C. Schoenstein
212-318-6273
richardschoenstein@paulhastings.com

Sandi F. Dubin
212-318-6648
sandidubin@paulhastings.com

San Diego

Mary C. Dollarhide
858-720-2660
marydollarhide@paulhastings.com

Christopher H. McGrath
858-720-2626
chrismcgrath@paulhastings.com

San Francisco

E. Jeffrey Grube
415-856-7020
jeffgrube@paulhastings.com

Kevin C. McCann
415-856-7064
kevinmccann@paulhastings.com

Stamford

Jay B. Worthington
203-961-7525
jamesworthington@paulhastings.com

Washington, D.C.

Kirby D. Behre
202-551-1719
kirbybehre@paulhastings.com

Jeremy P. Evans
202-551-1755
jeremyevans@paulhastings.com

Candice S. Shepherd
202-551-1801
candiceshepherd@paulhastings.com