

## **E-DISCOVERY AND AMENDED FRCP**

On December 1, 2006, a number of amendments to the Federal Rules of Civil Procedure went into effect. The amendments primarily addressed issues regarding the discovery of electronically stored information. Videos, digital pictures and images, emails, text messages, instant messages, website trails, temporary internet files, backup tapes, and flash drives all fall into this category. The amendments to the Federal Rules are critical because this type of information can be, and often is routinely, erased. This article will provide a brief summary of the amendments to the rules, address attorney/client privilege implications, and provide recommendations for clients aimed at preventing potential issues dealing with e-discovery.

### ***I. Summary of the Amended Rules***

The first major revision of the Federal Rules deals with planning electronic discovery. The amended rules encourage the parties to meet early and discuss issues related to the discovery of electronic information. Under Rule 26(f) the parties are required to hold a discovery-planning conference early on in the litigation. Specifically, it is to occur at least 3 weeks prior to the scheduling conference with the court. During this discovery planning-conference, 26(f) directs the parties to “discuss any issues relating to preserving discoverable information” and to develop a proposed discovery plan which addresses, among other things, “any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.” The hope here is that parties will communicate with each other regarding their e-discovery needs to prevent information loss.

Rule 26(f) works in tandem with Rule 16(b), which now provides that a court’s scheduling order may include “provisions for disclosure or discovery of electronically stored information” and “any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production.” According to the committee note, these amendments are intended to make courts aware of the need to lay out ground rules regarding the discovery of electronic information early on in the proceedings to avoid inadvertent spoliation. Furthermore, since the parties have already met and addressed the boundaries of e-discovery, as required by Rule 26(f), these issues should be ripe for discussion before the court at the time of the scheduling conference.

Under Rule 16(b)(6), a court can include in its scheduling order an agreement reached by the parties regarding assertions of privilege. The rule itself does not go into any further details. However, the committee note provides two illustrations of the type of agreements contemplated by the rule. First, the note refers to a “quick peek” agreement. Under a “quick peek” agreement, a producing party provides the requested materials for review. The requesting party then specifies the materials it desires to actually be produced. At this point, the producing party may assert a privilege or protection claim over the selected material. The purpose of the “quick peek” agreement is to make discovery more

efficient by requiring that the producing party only assert privilege or protection claims over selected materials, instead of having to screen all potentially discoverable material on the front end. Secondly, the note refers to a “clawback” agreement. Under a “clawback” agreement, the parties agree that the inadvertent production of privileged or protected materials does not constitute a waiver. Rather, the producing party timely notices the other party of the mistake, and the materials are returned. Again, this rule seeks to optimize discovery by obviating the need to spend copious amounts of time classifying documents before producing them.

The amendment to Rule 16(b) works together with the amendment to Rule 26(B)(5)(B), which provides the procedural steps that a party must take when privileged or protected information has been inadvertently produced. Prior to the amendment, Rule 26 did not address the steps that needed to be taken in such a situation. Under the new rule, the producing party must notify the recipient of the privilege or protection claim and the basis therefore. The recipient must then either return, sequester, or destroy the material pending determination of the issue by the court.

While Rule 26 provides the procedural steps that must be taken to preserve a privilege or protection claim, it does not determine whether the inadvertent production constitutes a waiver of the asserted privilege or protection. That is a matter to be dealt with under substantive law or by agreement of the parties. The latter approach is clearly favored by the recent amendments, as is evidenced by the ability for the parties to include an agreement—such as a “clawback” agreement or a “quick peek” agreement—in the scheduling order. Presumably, such an agreement will be controlling as to whether or not the inadvertent production constituted a waiver. Absent an agreement, the court would look to the applicable substantive law to make the determination.

Rule 26(a)(1)(B) now requires each party to produce, as part of its initial disclosures, a copy or description of electronically stored information that may be used to support its claims or defenses. In the new version of the rule, “electronically stored information” replaces “data compilations”, with the intent being to broaden the scope of the required disclosures.

Rule 26(b)(2) places needed limitations on the scope of discoverable electronic information. It provides that parties “need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.” However, this rule does not allow the producing party to avoid informing the requestor of the existence (or possible existence) of potentially discoverable information. The committee notes that the responding party must “identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing.” Additionally, the responding party is not relieved of its duty to preserve the evidence by simply identifying it as not reasonably accessible because of undue burden or cost. Rather, the responding party should take reasonable steps to preserve the information pending resolution of the matter. The intent of this rule is to exempt parties from time and resource consuming discovery “digs” if the information is not stored in a readily searchable format.

If parties cannot agree on the production of the information, the rule provides that it is to be resolved by way of a motion to compel or a motion for a protective order. On the motion, the party from whom discovery is requested must establish that the information sought "is not reasonably accessible because of undue burden or cost." Assuming this showing is made, the burden then shifts to the requesting party to establish "good cause" for production. Even if good cause is established, the rule leaves the decision to the discretion of the court.

Assuming the court orders production of the information, the rule also allows the court to "specify conditions for the discovery." This would include the ability to limit the amount of information produced and to specify the form of production. In an effort to deter overbroad requests, Rule 26 also provides the court with the discretion to order the requesting party to cover part or all of the costs of the production.

Rule 33(d) now specifically acknowledges that a party may produce 'electronically stored information' when answering an interrogatory. The rule allows a party the option to produce or make available for inspection the actual business record or an electronic equivalent. This option carries with it the onus that the responding party must make its electronic data available to the requesting party so it may deduce an answer to its interrogatory. This freedom carries with it implications of breaches of confidentiality. If there is a risk of a breach of confidentiality, the responding party may analyze the data itself and derive the answer, rather than using Rule 33(d).

Rule 34 addresses a party's requests for production of documents. Part (a) of the rule expands the traditional notion of inspecting physical documents by elevating electronically stored information to the same status as documents. Thus, the term "production of documents" now includes the inspection of electronically stored data. This rule requires the producing party to translate the electronically stored information into a reasonably usable form if necessary. It should be noted that the purpose of the rule is not to allow the requestor wild jaunts into the computer system of others, although such access may be necessary in some cases.

Part (b) outlines the procedure for responding to document requests. The rule gives the requesting party the option to designate the form or forms in which it desires the information produced. In the written response to the production request, the responding party must state the form in which it will produce the data if the requesting party has not voiced a preference or the responding party objects to the preference. As a catchall provision, the rule provides two default forms. The responding party must supply the information (1) in a form or forms in which the information is normally maintained, or (2) in a form or forms that are reasonably usable. This ensures that a responding party cannot convert the electronically stored data from its native form into a more complicated or burdensome form to impede the requesting party's discovery process. For example, if voluminous electronic data is normally stored in a searchable electronic format, the responding party should refrain from printing out the data and providing it in hard-copy format, as this may be deemed a form not reasonably usable.

Rule 37 outlines the sanctions for failing to make disclosures or cooperate in discovery. Electronic discovery poses the unique problem of spoliation to clients. Electronically stored information can be routinely modified, overwritten, or deleted in the ordinary course of business. Rule 37 recognizes data cleanup as a necessary part of managing an information system and creates a safe harbor for clients that inadvertently delete or purge discoverable material if that material was destroyed in the ordinary course of business. For example, if a business has a scheduled purge of information, they cannot be sanctioned for spoliation. This safe harbor, however, is limited by the bounds of good faith. “Good Faith” in this context means that a party is not permitted to simply stand by and allow the normal clean up procedures of the information system to wipe out discoverable information without consequence. To the contrary, this good faith component may require a party to modify or suspend routine operations to avoid data loss. This is termed a “litigation hold” on data cleanup procedures. It should be noted that this good faith requirement does NOT create a positive duty to preserve information, but more subtly the duty arises from common law, statutes, regulations, court order, or agreement between the parties.

## ***II. E-Discovery and E-Mail Privilege***

Parties to any lawsuit, attorney or client, need to be aware of privilege issues regarding e-mails. An individual e-mail often contains a series of ‘strings’ that entail several iterations of replies. This compilation of different ‘strings’ is often valuable in illustrating who knew what, and when they knew it. The natural approach is to classify an e-mail, containing multiple strings, as one document (i.e. the “1-document strategy”). Thus, if the e-mail contains privileged information, the entire document becomes non-discoverable. However, an argument can be that the ‘strings’ comprising the e-mail are actually several individual and different documents. Thus, a clever lawyer could argue for discovery of the non-privileged strings that make up the larger e-mail.

The implications of this ‘1-document strategy’ are many. For example, all documents claimed to be privileged must be entered into a privilege log, which is a document that describes the privileged information in enough detail to justify the privilege without revealing the contents of the document. The question becomes, under the 1-document strategy, how much detail is required when multiple strings are implicated? If the document is deemed to be logged incorrectly, the client is subject to sanctions which could include waiving the privilege and paying the opponent’s attorneys fees. Thus, a lawyer should be aware of the pitfalls of logging a string of e-mails as one document and likewise recognize the importance of efficiently and effectively logging privileged data.

This 1-document strategy was recently tested in *Universal Service Fund* where a defendant logged 35 e-mail strings, containing 131 separate e-mails, as single entries on its privilege log. *Universal Service Fund Telephone Billing Practices Litigation*, 232 F.R.D. 669 (D. Kansas 2005). The defendant argued that, due to the speed at which e-mail correspondence occurs, an e-mail was more akin to the transcript of a conversation, and therefore a single entry was appropriate. The

court found this argument unpersuasive and expressed concern that logging entries as a single document would prevent the opposing party from meaningfully challenging the invocation of privilege. While the court did not impose sanctions on the defendant, it did note in dicta that e-mail strings should be individually logged when claiming privilege. Ultimately, this issue is an open one, which will require today's attorneys to balance the burden of logging e-mails individually with the risk of sanctions.

### ***III. Cost to the Client***

The proliferation of e-discovery and its fruits bring with it an increase in cost of litigation for most businesses. For example, instead of simply reviewing hard-copy documents, lawyers must pour through sometimes unending stacks of e-mails looking for smoking gun evidence. In major cases this could mean several lawyers spending 12 hours a day reviewing and analyzing e-mails and attachments. This translates to a significant expense for clients.

One way clients can assist in this process is by investing in software to optimize this process. For example, software packages are available that automatically eliminate duplicate messages and can even link relevant messages together into discussion threads. This technology maximizes the use of attorney time and ultimately saves the client money. This type of software and other innovations are worth considering in light of the potential cost of litigation in today's electronic environment.

### ***IV. Recommendations***

The amendments to the Federal Rules foreshadow practical concerns that clients and attorneys must contemplate at the outset of any proceeding. For example, attorneys must remember to:

- Schedule an e-discovery conference with opposing counsel immediately after service of the citation, in the event that electronic data is at issue
- Log email strings separately when claiming privilege
- Ensure you are familiar with your client's data retention devices and the scheduled maintenance of those devices

Similarly, clients have a responsibility to:

- Be familiar with your company's electronic data maintenance schedule – know when emails and documents are purged and archived
- Create an electronic document retention policy – this is your best defense against spoliation sanctions
- Develop a litigation hold policy
- Create channels of communication between the legal department and the IT department to facilitate production of e-materials and to initiate litigation holds
- Make it a known company policy that employees are not to delete e-mails, documents, or any other electronic information that could contain discoverable material