

Electronically Stored Information and the Federal Rules of Civil Procedure

Last December, the U.S. Supreme Court approved a number of significant changes to the Federal Rules of Civil Procedure (FRCP), which regulate the discovery of electronically stored information (ESI).¹ The amendments provide a framework for conducting electronic discovery, obliging litigants to identify, preserve, and collect ESI very early in a case. The amendments affect all computer systems used by higher education institutions that may become involved in litigation in federal courts.

ESI can be found in e-mails, voice-mails, instant messages, text messages, documents, spreadsheets, databases, file fragments, metadata, digital images, and digital diagrams. It can be stored in every type of electronic media including hard drives, thumb drives, computers, handheld devices, backup tapes, and optical disks. The ease with which ESI can be generated, stored, altered, transmitted, and destroyed has complicated the discovery process, as has also the sheer volume of information that is processed and the various formats in which it can be created, stored, and produced.

Colleges and universities that do not actively manage their ESI may face difficulties in compliance, increased risks of sanctions, and higher litigation costs. A quick synopsis of several of the relevant amended rules is provided below, followed by suggested ESI management practices.

Early Attention to ESI

The new Rule 26(f) requires parties to meet early in the litigation process and confer about discoverable ESI and issues

related to it. During this initial meeting, parties will discuss the discovery plan, which includes the following: (1) what ESI will be relied on by the litigants; (2) how each party stores its ESI; (3) in what form the information will be produced; (4) the accessibility of the information; and (5) issues related to privileged ESI.

The necessity for proficient ESI management becomes evident at this initial meeting. Attorneys for the litigants are responsible for knowing the details of their clients' information systems and retention policies. They will also need to know the ESI that their clients will rely on for claims or defenses and whether that ESI is accessible or potentially contains privileged information.

Classifying information as "litigation sensitive" or "privileged" and indexing it for search and retrieval are information management steps that will help in this phase of litigation. Knowing where information is stored and processed not only will assist in keeping costs down but also will offer an advantage by providing some certainty when responding to the initial questions posed pursuant to Rule 26(f). The agreement made by the parties under Rule 26(f) will be adopted in a court order following a Rule 16(b) pretrial conference. Therefore, it is important to be able to answer these preliminary questions with some certainty.

Privileged Information

The protection of privileged and confidential information, such as information protected by the attorney-client relationship, is especially difficult due to the volume of ESI. Although parties are to discuss potential privileged and confi-

dential information early in the litigation process, the inadvertent disclosure of this information during discovery may result in privilege waiver (making the information discoverable).

Rule 26(b)(5)(B) has been amended to address the inadvertent production of privileged information. Under this rule, the producing party must immediately notify the receiving party of the inadvertent disclosure of privileged information, and the receiving party must promptly return, sequester, or destroy specified information in any copies it possesses. This information may not be used by the receiving party until the claim is resolved by the court; however, the receiving party may provide a copy of the privileged information to the court under seal, so that the information may be reviewed as to the privilege claim.

ESI must be managed so that privileged information is identified and protected. This includes storing privileged information in a secure location and indexing it for search and retrieval. It also calls for a method for searching ESI so that privileged information can be identified and removed. A second, more thorough review of produced ESI will be required in order to invoke the procedures included in this rule.

Reasonable Accessibility

As amended, Rule 26(b)(2) permits parties to avoid discovery of ESI if the information is not reasonably accessible due to undue burden or cost. Although the phrase "reasonably accessible" is not defined by the FRCP, case law has provided some guidance. Information in readily usable formats will be deemed

“reasonably accessible.” This includes the information on active hard drives, servers, and disks that are readily accessible. It also includes systematically organized and easily retrievable backup tapes or disks. Data that is not reasonably accessible includes electronic information that has to be converted or recovered in order to be usable. This typically includes data backup tapes that are not systematically organized or indexed and data that is deleted, damaged, or fragmented.

The party requesting the information that the responding party designated as not reasonably accessible is permitted

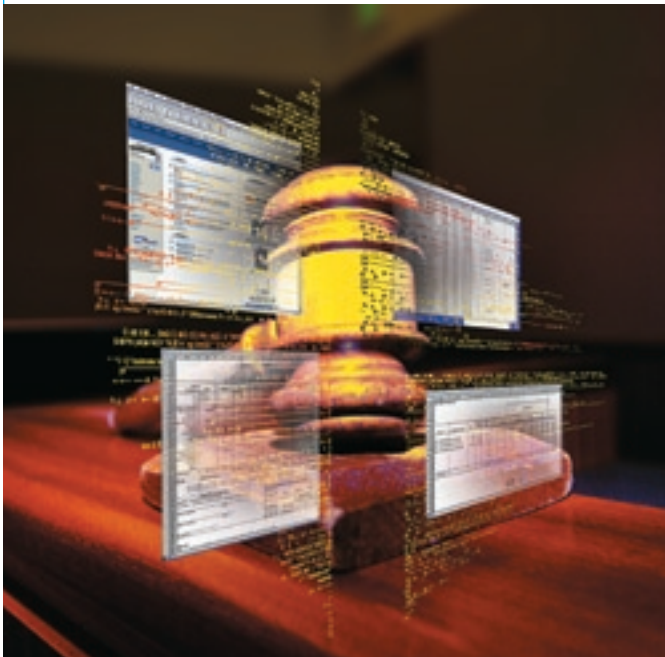


Illustration by Ron Brown, © 2007

to seek discovery to evaluate the claim of inaccessibility. If challenged by the requesting party in a motion to compel production, the responding party has the burden of establishing that the data is not reasonably accessible. If no showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause and is willing, among other possible conditions, to bear the cost of accessing the data.

From a producing party's standpoint, having data readily accessible will lower litigation costs. So, the foregoing ESI management steps will also be helpful under this rule. When seeking information, an institution should have sophisticated computer forensic capabilities to counter the producing party's claims that the data being sought is inaccessible and not subject to discovery.

Forms of Information

Rule 34(b) provides that ESI is to be provided in a form in which it is ordinarily maintained or a form that is readily usable. If the requesting party specifies another form in which the ESI is to be produced, the producing party has the option to object to the requested form and propose its own form in which the ESI is to be produced. The rule provides dispute-resolution procedure if the parties cannot agree.

Good ESI management will require ESI to be kept in a readily usable form or, at a minimum, in the form in which it is ordinarily maintained. For example, organizations that image paper documents and completely replace them with electronic documents in PDF and TIFF formats not only will enjoy superlative information-management capabilities but also will be better able to handle litigation. Imaging affords advanced indexing and searching capabilities. Turning word-processing

files into imaged documents removes metadata. Destruction of paper documents will lessen litigation costs. The ordinarily maintained resulting images will fully comply with Rule 34 (b), since they will be ordinarily maintained in a usable format.

Receiving parties should have knowledge about their systems capabilities and the form of the ESI that can be used by them. This information should be gathered as early as possible in the discovery process.

Safe Harbor

Lawyers have a duty to preserve evidence relevant to actual or potential litigation. There are numerous examples of courts that have imposed sanctions for *spoliation*, a term describing when a party fails to produce information that has been

wrongfully destroyed. The amended Rule 37(f) provides that the court may not impose sanctions when a party destroys ESI as part of its “routine, good faith” operations. This “safe harbor” is one of the strongest reasons for a college or university to include an ESI retention and destruction program in its ESI management program.

Written ESI retention policies, coupled with evidence that the policy is routinely followed, are essential to show that the destruction of the information was in good faith. Since the safe harbor provision will not protect a party if ESI was destroyed in anticipation of litigation, procedures should also be drafted to place a “litigation hold” on all potentially relevant ESI. An effective litigation hold procedure provides notice to all the relevant people in an organization as to what must be retained and for how long. Reminders and updates about the litigation holds should be circulated periodically.

Conclusion

The FRCP provide some clarity in how ESI will be handled during discovery. They also affect how organizations will manage the vast amount of ESI created, stored, used, and retrieved. Colleges and universities can prepare by identifying the information that is most relevant to their litigation needs and by beginning to take steps to manage their ESI, such as categorizing, indexing, and storing it in a way that will make it searchable and readily accessible. ESI should be routinely destroyed in accordance with written policies when it is no longer legally or operationally required. Litigation hold procedures should also be prepared. Finally, all other policies and procedures—such as those related to e-mail, privilege protection, security, and privacy—should be reviewed and updated as necessary.

Note

1. Amended were Rules 16, 26, 33, 34, 37, and 45 and Form 35.

M. Peter Adler (JD, LL.M., CISSP, CIPP) is President of AIPG LLC and is the Interim Director of Privacy and Cybersecurity at Montgomery College and formerly the Information Security Officer at the University of Colorado.

