CHANGES TO THE FEDERAL RULES OF CIVIL PROCEDURE BRING eDISCOVERY ISSUES TO THE FOREFRONT

BY THOMAS R. GOOTS AND KARL M. MAERSCH

Ten years ago, a party involved in a major piece of patent litigation might expect to produce 300 boxes full of documents. Today it is conceivable that the same party in the same litigation could produce the equivalent of 300 semitrailers full of documents. Though we all benefit from, and take advantage of, the availability of electronic information and communication, these innovations can create nightmares for a company involved in patent litigation. The Federal Rules of Civil Procedure have recently been amended to address electronic information. Knowing the scope of those changes and following some basic steps will help to ensure that parties do not run afoul of the amended rules.

On December 1, 2006, the Federal Rules of Civil Procedure were amended to specifically address eDiscovery issues. These rule changes were brought about by the realization that the discovery of electronic information presents problems which the discovery of paper documents did not. The revised rules explicitly refer to electronic data, which requires parties and the court to deal with these issues head-on, often at the outset of the case. This article provides an overview of the rule changes and contains a discussion of how to cope with the revised rules as a litigant.

ADVISORY COMMITTEE ON CIVIL RULES INVESTIGATES PROBLEMS WITH eDISCOVERY

At a conference in 1996, the Advisory Committee on Civil Rules (the "Committee") was advised of problems with computer-based discovery. The Committee set out to revise the rules in 1999. Between 2000 and 2004, the Committee sought input from bar organizations, attorneys, computer specialists, judges, and litigants regarding potential changes to the rules to deal with problems created by electronic documents and information.

Based on the input that was received, the Committee determined that there were three main differences between electronic information and paper documents. First, the volume of electronically stored information was exponentially greater than that of hard-copy documents. The Committee noted that large organizations maintain computer networks that can store terabytes of information, with one terabyte representing the equivalent of 500 million pages. In addition, the Committee noted that large organizations receive 250 to 300 million e-mail messages per month.

The second difference between electronic information and paper documents was that information stored electronically is subject to automatic processing by computers, which can overwrite or delete information as part of normal operation, often without the input (or even the knowledge) of the user. This creates issues regarding document destruction and document accessibility that the Committee needed to address. Third, the Committee recognized that electronic information can be incomprehensible when separated from the system or software that created it, which creates issues regarding accessibility.

Based on these three findings, and coupled with the fact that its study had shown that dealing with the discovery of electronic information was becoming more costly, burdensome, and time-consuming, the Committee determined that revisions to the Federal Rules of Civil Procedure were needed to address computer-based discovery. The revised rules were approved by the Supreme Court in April 2006 and went into effect on December 1, 2006.

THE REVISED FEDERAL RULES AFFECTED SEVEN ASPECTS OF DISCOVERY

The changes to the Federal Rules can be grouped into seven main topics. First, the rules now explicitly provide for the discovery of computer-based information. Prior to the amendments, courts treated electronic documents and information as being within the definition of "data compilations" in Rules 26 and 34 and handled discovery of these materials in the same manner as that of paper documents. The revised rules provide for the discovery of "electronically stored information," which is defined as "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained." This differentiates discovery of electronic information from that of paper documents.

Second, revised Rule 26(f) requires the parties to discuss eDiscovery issues at the Rule 16 conference, which generally occurs soon after the defendant has filed its answer. At a minimum, the parties should discuss preserving discoverable information, disclosure of what electronically stored information each party has, the form of production for electronically stored information,

The revised rules explicitly refer to electronic data, which requires parties and the court to deal with these issues head-on, often at the outset of the case.

and the consequences of inadvertent disclosure of privileged information. According to the Committee Notes to the revised rules, the purpose of these changes is to force the parties to discuss electronic discovery issues early in the case in order to minimize difficulties and disputes later.

Third, the revised Federal Rules invite the parties to reach agreements concerning privilege. According to the Committee Notes to Rules 16 and 26, this is a recognition that the amount of electronic data that must be reviewed prior to production can cause delay and expense as the parties try to avoid risk of waiver of a privilege. The Notes specifically mention "quick peek" agreements, where the responding party produces files for inspection without waiving privilege, and "clawback" agreements, where the receiving party must return any information that is later determined to be privileged.

Fourth, the requirement to produce electronic data focuses on whether the data is reasonably accessible. According to Rule 26(b)(2)(B), data from sources that are "not reasonably accessible," because of undue burden or cost, need not be produced. The revised rule codifies current case law that allows a requesting party to obtain discovery of data that is not reasonably accessible if "good cause" is shown. In that instance, however, the court may shift the costs of making the data accessible from the producing party to the requesting party. The accessibility of data often turns on the media on which it is stored. Examples of "accessible data" are active, online data stored on drives and near-line data stored on optical disks. Examples of "inaccessible data" are backup tapes intended for disaster recovery, legacy data remaining from systems no longer in use, and deleted data that remains in fragmented form.

Fifth, the revised rules allow the requesting party to specify the format of production for electronically stored information. Revised Rule 34(b) allows the responding party to object to the requested form, but the data must be produced in a form that is "ordinarily maintained" or "reasonably usable." A party should expect that if the data on its system is in searchable format, the party seeking discovery of that information will request that it be produced in the same searchable format.

Sixth, the revised rules address sanctions for the destruction of electronically stored information. Revised Rule 37(f) provides a safe harbor for information lost as a result of the routine, good-faith operation of an electronic information system. This change is intended to recognize that a distinctive feature of computer systems involves the routine modification, overwriting, or deleting of information in normal use. With respect to this revision, the Committee Notes provide that whether good faith exists will depend on factors such as the reasonableness of the litigation hold on document destruction put in place by the party, the steps taken to comply with a court order, and the steps taken to comply with the agreement of the parties on preservation. However, a party is not permitted to exploit routine operation of a computer system in order to destroy potentially relevant data.

Seventh, revised Rule 45 applies all of the changes discussed above regarding discovery between parties, such as accessibility, privilege, form of production, and destruction issues, to subpoenas issued to nonparties.

THE DUTY TO PRESERVE DISCOVERABLE INFORMATION

While many of these rule changes impact aspects of discovery normally handled by outside counsel, several areas of change point to the need for companies to have an understanding of how their data is stored, backed up, and deleted. An understanding of where the company's data exists and for how long will ensure that the company preserves discoverable information and is not left open to sanctions for the destruction of electronically stored information.

Under existing case law, the duty to preserve discoverable information arises when relevant people at the company reasonably anticipate litigation. In addition to the common-law duty to preserve evidence, a company may have a statutory or regulatory duty to preserve data, even before litigation is reasonably anticipated. For example, the Securities and Exchange Commission requires e-mails on certain subjects to be retained for a number of years. The scope of the duty to preserve evidence extends to all individuals at the company who are likely to have discoverable information.

A document retention policy, document destruction policy, or records management policy is a framework by which companies manage the collection, retention, and eventual routine destruction of information. These policies typically address how long electronic documents and information are retained and by what method. Such policies also provide for whether and how often particular kinds of information are backed up.

For reasons that will become apparent, it will be important to immediately notify the company's information technology ("IT") department as soon as litigation is anticipated. Computer systems can automatically delete electronically stored documents and information or can delete it at certain specified times. In order for a litigant to comply with its duty to preserve discoverable information, the document retention policy must be suspended whenever litigation is anticipated. For example, a program that automatically deletes e-mails that are older than 60 days must be suspended for those e-mails that are potentially relevant to the anticipated litigation. In addition, the automatic maintenance of hard drives and servers including defragmenting, formatting, or wiping must be suspended where those processes would affect information that would be discoverable in the anticipated litigation.

An issue that remains open is to what extent the duty to preserve data extends to backup tapes. Case law that predates the revised rules suggests that the duty does not extend to backup tapes that are not reasonably accessible unless a company can identify which backup tapes contain data from "key players." The revised rules, however, appear to contemplate that parties retain all backup tapes, in that the Committee Notes provide that the mechanism for determining whether something is not reasonably accessible is for a party to move for a protective order.

EFFECTIVE DISSEMINATION OF A LITIGATION HOLD

Once a company anticipates litigation, it should immediately contact counsel familiar with litigation and the revised rules, whether outside or in-house, to develop a "litigation hold." A litigation hold, or "document retention alert," is a notice sent to all company employees who are likely to have information relevant to the anticipated litigation. The notice should identify the scope and type of information to be retained and provide a mechanism for retaining the information. In order to be effective, the notice should come from a source whose directive is likely to be followed, such as a combination of senior department heads and the legal group. As discussed above, the notice must also be sent to the company's IT department.

Moreover, the notice should be periodically redistributed to key players and to the IT staff during the course of the litigation so that employees in possession of potentially relevant information are reminded of their duty to preserve it. In addition, it is good practice to check that the data is being retained. This would involve following up with key employees and the IT department. While it is nearly impossible to ensure that every shred of paper, every e-mail, every file, and every backup tape is retained, the goal is to show the court that the company took immediate, appropriate, and thorough steps to preserve evidence relating to the anticipated litigation.

To the extent that the litigation hold does not prove effective and electronically stored information is lost, revised Rule 37(f) provides a safe harbor from sanctions with respect to information lost as a result of the routine, good-faith operation of an electronic information system. The Committee Notes to the rule provide that factors that bear on whether there was good faith are the reasonableness of the litigation hold, the steps taken to comply with a court order where the party has already been compelled to produce information, and the steps taken to comply with an agreement the parties have reached concerning preservation of documents and information. Even before the rule changes, courts found that a company's failure to impose a litigation hold was irresponsible and a factor to consider when assessing whether intentional destruction had occurred.

CONCLUSION

Electronically stored documents and information are here to stay. The revised Federal Rules reflect a recognition that discovery must change to account for all forms of electronic data. A document retention policy that puts the company in control over what information it maintains, how long it maintains that information, and the form in which the information is maintained is imperative. It keeps the amount of electronic documents and information in check. In addition, it is essential that a litigation hold that properly preserves the potentially relevant paper and electronic documents and information be put in place as soon as the company anticipates litigation. Finally, involving outside counsel as soon as litigation is anticipated is a good way to ensure sanctions-free compliance with the revised rules. ⏭

THOMAS R. GOOTS
Cleveland ‖ 1.216.586.7011 ‖ trgoots@jonesday.com

KARL M. MAERSCH
Cleveland ‖ 1.216.586.7032 ‖ kmmaersch@jonesday.com