

## **New U.S. Rules of Civil Procedure**

Recent amendments to the U.S. Federal Rules of Civil Procedure have put into focus the importance of managing and preserving of electronically stored information.

Given changes to the US Rules in December 2006, corporate data risk management programs in any international organisation must now be designed to do more than prevent and respond to information security breaches and network disaster scenarios. Now businesses in the UK and Europe must also prepare for the fact that information may become subject to discovery in U.S. legal matters.

The changes—which affect Rules 16, 26, 33, 34, 37 and 45—were enacted to reflect the reality of electronic discovery in modern litigation. In light of these rule changes, businesses are increasingly recognising that a failure to safeguard the integrity of electronically stored information (“ESI”) can also give rise to legal liability. Indeed, the provisions apply to any entity that is called upon by a US federal court to provide discovery for litigation.

To ensure compliance with the obligations outlined in the U.S. Federal Rules of Civil Procedure (“FRCPs”), IT departments and CIOs in the UK must develop and employ comprehensive, enterprise-wide solutions for managing ESI.

### **Key Rule Changes**

The amendment to Rule 34(a), which expressly recognizes ESI as a type of discoverable information, is a deceptively modest change. While the rule had previously allowed for the discovery of “data compilations,” the amended rule specifically directs that parties may obtain discovery of “electronically stored information,” including data compilations “stored in any medium from which information can be obtained.” Thus, the revised language answers any lingering question as to whether discovery extends to all forms of electronic documents and data in the affirmative. With this single vernacular update, the rule ensures requesting parties are afforded an opportunity to obtain ESI during discovery, while definitively putting would-be producing parties on notice of their corresponding preservation obligations.

This is especially significant in light of the risk of spoliation sanctions (the failure to preserve discoverable documents, whether intentionally or merely negligently despite notice of a discovery obligation). This can give rise to a host of penalties, including unfavorable jury instructions and monetary fines—a harsh reality underscored in recent high-profile U.S. cases such as Morgan Stanley, Zubulake and Philip Morris.

Recognising that ordinary business practices ought not to be unduly hampered by the prospect of potential litigation, the FRCP changes also include a provision aimed at limiting sanctions for a party’s inability to produce ESI lost as a result of “routine” data management practices that are carried out in “good-faith.” However, the so-called “safe harbor from sanctions” provided by Rule 37(f) offers limited protection. Rule 37(f) only limits sanctions issued pursuant to the Federal Rules of Civil Procedure; it does not alter the court’s ability to impose sanctions derived from inherent or other sources of authority. Moreover, even when information is lost due to a party’s “good-faith routine operation of a computer system,” the amendment allows for sanctions under the Federal Rules in “exceptional circumstances.”

Additions to Rule 45(d) clarify that most of the discovery provisions provided in the FRCPs extend to subpoenaed and party respondents alike. Businesses who fail to preserve discoverable documents and data after subpoena may be found in contempt of court pursuant to Rule 45(e), or liable for spoliation. Accordingly, good data housekeeping should not be seen only as a job for plaintiffs and defendants. Businesses at risk of being subpoenaed for ESI in their possession or control are wise to follow the same data management practices suggested for litigants.

### **IT’s Role in Planning for E-Discovery & Averting Sanctions: Best Practices**

In light of the risk of sanctions and limited protections afforded by Rule 37(f), businesses should ensure document destruction activities are only carried out as part of a defensible, ongoing document management program. A favorable step toward demonstrating “good-faith” in the “routine operation” of an information system—and minimising the risk of sanctions—is the creation and use of a litigation response team. The litigation response team should include members from outside counsel, in-house counsel, IT, records management, compliance, and other departments relevant to the litigation in question.

When litigation arises a response team is critical to ensuring suspension of routine destruction practices that may otherwise compromise the organization's preservation obligations. This includes ensuring that any backup media containing potentially pertinent data is identified, segregated and stored in a safe place. Other sources of discoverable information should also be identified and safeguarded.

While the litigation response team should have the support of upper level management, the most important members of the litigation response team are often corporate IT specialists who understand the relevant information management policies of the organization and the extent to which those policies are actually followed. Working together, counsel and IT staff should determine what data needs to be preserved, how to implement a preservation hold and how to monitor compliance with preservation protocols. To streamline those efforts corporate IT staff should be sure to convey the following information to counsel:

- All the storage areas, including all geographic locations that might contain relevant evidence;
- All current and former personnel (including those with remote network access via home computers and laptops) that may possess relevant information;
- All the operating systems and software applications (current and historical) that contain potentially responsive data;
- All hardware formerly and currently in use;
- Disk or tape labeling conventions, file name customs, location-saving rules;
- Types of data that will need to be restored from backup tapes, the age of those tapes, their location and the frequency with which they are recycled;
- An explanation of your corporate document retention policy and the current enforcement status of that policy; and
- Corporate policies regarding employee use of company computers and data.

To ensure ESI that may be pertinent to the litigation in question can be promptly identified, IT staff should also create and maintain a directory of the business' information systems before litigation is even contemplated. A data storage directory should include:

- Records of all types of hardware and software in use and the locations of all electronic data, and
- A map outlining the flow of data into and out of the company.

In addition to conveying critical information about the company's document retention policies, backup tape recycling schedules, and system architecture, IT staff should also facilitate lines of communication between counsel and electronic discovery experts. Working with counsel and IT, these experts are critical for managing the collection of ESI and facilitating review and production of responsive data should litigation occur.

IT staff should not, however, be relied on - in place of an experienced electronic discovery provider - to handle an electronic discovery project from preservation through production. Corporate IT is unlikely to have the bandwidth to collect, analyse, organise, and prepare ESI for review in legal matters while keeping current systems running.

Notwithstanding the strain on IT resources, it is also unreasonable to place the responsibility of managing the evidentiary integrity of ESI on IT professionals who have not received the training to do so. In the event that a party's gathering, sorting, filtering or production processes are called into question, the individuals charged with carrying out these tasks may be called as witnesses to explain and justify their efforts. While IT professionals may be more than qualified to testify as an expert about a company's technology and infrastructure, they should not be expected to testify as an expert on legal technology issues.

Finally, businesses that opt not to engage a qualified electronic discovery provider in spite of their lack of internal resources and expertise place themselves at an even greater risk for sanctions. For example, in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.* when the defendant, Morgan Stanley, mishandled ESI pertinent to the litigation, the court specifically admonished the corporation for giving "no thought to using an outside contractor to expedite the process of completing the discovery, though it had certified completion months earlier; it lacked the technological capacity to upload and search the data at that time, and would not attain that capacity for months." Finding, numerous instances of discovery misconduct, the court ordered a jury instruction that was adverse to the defendant, noting "[t]he conclusion is inescapable that [the defendant] sought to thwart discovery." In May 2005, relying in part on that instruction, the jury awarded \$1.45 billion in total damages against Morgan Stanley.

## **Conclusion**

The U.S. FRCP amendments serve as yet another reminder of the myriad challenges of managing corporate data. In England and Wales, recent amendments to the Practice Direction under the Civil Procedure Rules (CPR) r 31 also clarify that electronic documents are subject to disclosure in civil matters. As U.K. courts begin interpreting these provisions, electronic discovery is likely to become an increasingly important aspect of enterprise risk management. CIOs, Corporate IT departments and legal counsel are working together to assess their companies' electronic disclosure liabilities and to formulate appropriate data preservation, searching and production plans. These steps are critical to minimising data management mishaps and protecting businesses from the risk costly discovery mistakes.

**About the author**

Amanda J.G. Karls, Esq. is a staff attorney for Kroll's legal technology division in Eden Prairie, Minnesota