

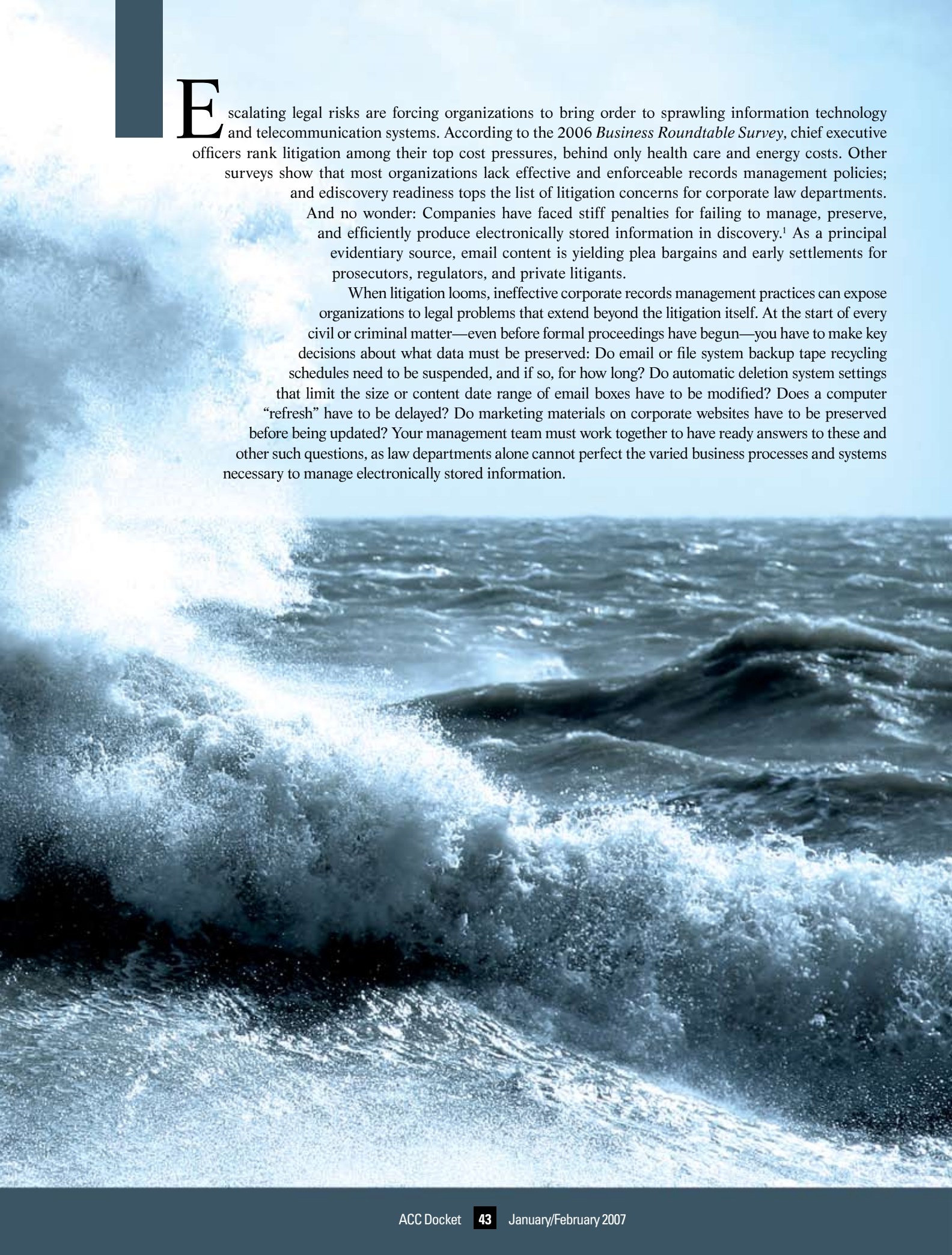


**R**OUGH  
**W**ATERS

# **AHEAD**

**for Ediscovery and the New Federal  
Rules of Civil Procedure**

By Beryl A. Howell and Richard J. Wolf



**E**scalating legal risks are forcing organizations to bring order to sprawling information technology and telecommunication systems. According to the 2006 *Business Roundtable Survey*, chief executive officers rank litigation among their top cost pressures, behind only health care and energy costs. Other surveys show that most organizations lack effective and enforceable records management policies; and ediscovery readiness tops the list of litigation concerns for corporate law departments.

And no wonder: Companies have faced stiff penalties for failing to manage, preserve, and efficiently produce electronically stored information in discovery.<sup>1</sup> As a principal evidentiary source, email content is yielding plea bargains and early settlements for prosecutors, regulators, and private litigants.

When litigation looms, ineffective corporate records management practices can expose organizations to legal problems that extend beyond the litigation itself. At the start of every civil or criminal matter—even before formal proceedings have begun—you have to make key decisions about what data must be preserved: Do email or file system backup tape recycling schedules need to be suspended, and if so, for how long? Do automatic deletion system settings that limit the size or content date range of email boxes have to be modified? Does a computer “refresh” have to be delayed? Do marketing materials on corporate websites have to be preserved before being updated? Your management team must work together to have ready answers to these and other such questions, as law departments alone cannot perfect the varied business processes and systems necessary to manage electronically stored information.

But help is on the way...or is it? The amendments to the pretrial discovery rules of the Federal Rules of Civil Procedure, enacted after almost five years of work and consideration of public comments, are supposed to clarify how to handle electronically stored information (ESI). The drafters acknowledged that the old discovery rules “provide[d] inadequate guidance to litigants, judges, and lawyers in determining discovery rights and obligations in particular cases.”<sup>2</sup> Anticipating the new amendments, one federal district court judge was “optimistic” that “counsel will heed the guidance provided by these resources and will work to ensure that preservation, production and spoliation issues are limited, if not eliminated.”<sup>3</sup> The unfortunate reality, however, is that these new rules of procedure are likely to stimulate a new breed of complex discovery disputes.

### The Amendments to the FRCP

The changes to the federal rules of discovery address three critical areas that have increasingly become the fodder for costly and distracting ediscovery disputes:

- the timing and types of disclosures about ESI required of parties;
- absent an agreement between parties, “default” formats for production of ESI and procedures for protecting against inadvertent disclosure of privileged communications and attorney work product; and
- new limitations on the scope of searches for potentially relevant ESI, accompanied by a new and controversial rule that could protect parties from sanctions if they lose ESI.

It is important to note that these rules are procedural, not substantive, and the amendments, therefore, do not prescribe legal duties on preserving ESI, whether or not reasonably accessible. The development of federal common law principles will shape these duties. Nor do the amended rules address important substantive questions concerning privilege waiver in the handling of ESI.<sup>4</sup>

This article focuses on two principal aspects of the changes to the federal rules: new requirements to make disclosures about ESI at the outset of every lawsuit; and a so-called sanctions bar intended to protect parties who lose ESI from the “routine, good-faith” operation of IT systems. In both cases, the amended rules may, despite the drafters’ good intentions, introduce more complexity to federal civil litigation than the rules resolve.



BERYL A. HOWELL is a partner of Stroz Friedberg, LLC, a technical services and consulting firm specializing in digital forensics, electronic discovery, and cybersecurity investigations, and a commissioner on the US Sentencing Commission. She may be reached at [bhowell@strozllc.com](mailto:bhowell@strozllc.com).



RICHARD J. WOLF is president of the Association of Corporate Counsel’s Greater New York Chapter and was head of global compliance at Candant Corporation until the corporation’s disaggregation in 2006. During his decade as an executive in the law department, Wolf brought legal and business-process innovation to Candant (and its predecessor HFS Incorporated), helping the corporation become a model of streamlined and effective compliance, litigation, and records management systems. He may be reached at [rwolf@lexakos.com](mailto:rwolf@lexakos.com).

The views expressed herein are those of the authors alone.

### The New Ediscovery Disclosure Requirement

The accumulation of email and other forms of ESI, such as spreadsheets, presentations, and other documents, is not a new predicament for organizations, but the new rules are forcing businesses to begin to address the problem. These amendments obligate parties to make initial disclosures about ESI, before receiving a specific discovery request, by providing the other side with “a description, by category and location of, all...electronically stored information...that are in the possession, custody, or control of the party...” And, for the first time, amended Rule 26(f) requires parties to meet and confer about specific issues relating to the preservation, searching, and production of ESI, whereas previously, parties were only required to discuss discovery of “documents” and “tangible things” at the discovery conference.

This new concentration on ESI is raising issues that you and your outside counsel may not be fully prepared to address, especially at the outset of litigation. Among other new areas for consideration, parties must be prepared to defend or provide evidence on:

- how and where your company stores ESI—Rule 26(a)(1)(B) (initial disclosure of categories and location of ESI));
- an assessment of the relative accessibility of ESI from different sources, including the time and cost of retrieving the data for review—Rule 26(b)(2)(B) (relieving parties of the need to provide ESI from sources identified as

- not reasonably accessible due to undue burden or cost));
- the “routines” or policies in effect for records management and business functionality that may have to be interrupted or suspended to preserve ESI—Rule 26(f) (discussion of issues related to preserving discoverable information); Rule 37(f) (possibly protecting parties from sanctions for data lost due to routine, goodfaith operation of electronic information systems);
- the format or formats in which ESI is created and stored, and the format to be used for production—Rule 34(b) (allowing requesting parties to specify the form in which to produce ESI); and
- search protocols used to identify responsive and nonprivileged information—Rule 26(f)(1)–(4) (encouraging parties to stipulate plans for discovery of ESI, including timing, phasing, preservation scope, production

formats, and procedures for handling privileged material.<sup>5</sup> Curiously, the new rules expect outside counsel to grasp these technical areas and frame cogent legal arguments involving corporate IT practices *before* conferring with adverse parties. Moreover, lawyers are constrained to make early judgments about whether to declare certain data “not reasonably accessible” by invoking new procedures in Rule 26(b)(2)(B) to contest the scope of discovery based on arguments of “undue burden or cost.” Expect extensive motion practice challenging the adequacy of evidence, arguing undue burden or cost, and cross motions for protective orders based on notions of fairness and good faith. Since ESI may include voicemail, deleted data, temporary files, system history files, website information, cache files, and other data that is not routinely and easily retrievable by the normal computer user, the list of reasonably inaccessible data subject to discussion—and contention—may grow large.

This new ediscovery frontier is giving headaches to district court judges, magistrate judges, and parties called upon to referee or litigate disputes. The new rules promise to increase the use of special masters, mediators, and other third party specialists to resolve disputes about the costs and burdens associated with the storage and retrieval of ESI. For these reasons, organizations increasingly seek expert analysis from professionals experienced in meshing IT systems with legal preservation requirements, since factually unsupported assertions of undue burden and cost “can be expected to fail.”<sup>6</sup>

To survive motions to compel production of ESI and avoid monetary penalties, adverse inference charges, and a litany of other undesirable consequences, companies will need to bring order quickly to a historically chaotic area—namely, the management of email and other ESI. There is hope, however, for those few organizations ready to answer where, when, what, and how data are stored for discovery purposes.

### **A New Sanctions Safe Harbor?**

A new subsection has been added to Rule 37 for situations where a party fails or is unable to provide ESI in discovery. The rule now provides:

**Rule 37(f) Electronically Stored Information.** *Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.*

At first blush, many view Rule 37(f) as a “safe harbor,” but allusion to the new rule as such would be a misnomer. The rule does not relieve a party from the common law duty to preserve evidence or the new requirement to identify ESI sources that “are not reasonably accessible

## **ACC’s Policy on Ediscovery**

ACC supports proposals that presumptively limit the need to preserve and produce information that would otherwise be rendered inaccessible under regular records retention policies and procedures. Current rules are unclear, providing too much latitude for discovery abuse, especially affecting companies that have properly purged or recycled documents under reasonable corporate records retention or disaster recovery policies. Additionally, ACC strongly supports proposals that would provide a “safe harbor” from sanctions for the routine loss of information that can occur despite good faith operation of a conventional records system.

ACC’s policy regarding ediscovery can be found at [www.acc.com/public/accapolicy/ediscovery.pdf](http://www.acc.com/public/accapolicy/ediscovery.pdf).

### **ACC Comment Letter on Rule 502 and the Ediscovery Guidelines**

In June 2006, ACC, on behalf of its members, filed comments on Proposed Rule 502 concerning limited waiver protections for organizational entities against third party discovery of attorney-client privilege and work-product protected documents, and communications with the Standing Committee on Rules of Practice and Procedure of the Judicial Conference of the United States.

ACC’s comment letter can be found at [www.acc.com/public/attyclientpriv/502acc.pdf](http://www.acc.com/public/attyclientpriv/502acc.pdf).

because of undue burden or cost.” Thus, before relying on Rule 37(f) as a means to defeat a motion for sanctions, your organization must have its IT house in good order—otherwise it will be unable to satisfy key elements of Rule 37(f) and demonstrate the loss of information through the “routine” operations. Unfortunately, recent studies indicate that most organizations do not have routines built on effective records management compliance programs or a firm grasp on the management of current or legacy systems with ESI. If yours is among those who need better policies and procedures, you may find Rule 37(f) more useful as a cudgel to establish an effective and properly resourced records management compliance program. The areas requiring attention for application of Rule 37(f) are discussed below.

### **“Routine” Operations**

To avoid sanctions under Rule 37(f), the loss of electronic data must be the result of the “routine operation” of an electronic information system.<sup>7</sup> Yet ever-changing,

## ACC Extras on... The New Federal Rules of Procedure and Ediscovery

### Webcasts:

The following ACC webcasts are available.

- Spring Cleaning: Steps to Reduce Electronic Discovery Costs Under the New FRCP Amendments: [www.acc.com/resource/v6804](http://www.acc.com/resource/v6804). Transcript for this webcast can be located at: [www.acc.com/resource/v7154](http://www.acc.com/resource/v7154)
- Planning for the New Federal Rule Changes. Transcript for this webcast can be located at: [www.acc.com/resource/v7251](http://www.acc.com/resource/v7251)

### ACC Top Ten:

- Top Ten Tips for Corporate Counsel in Dealing with the New FRCP on Ediscovery: [www.acc.com/protected/reference/tech/ediscovery.pdf](http://www.acc.com/protected/reference/tech/ediscovery.pdf)

### ACC Alliance:

The following ACC Alliance partner offers records enforcement services. To receive your ACC discount, be sure to mention that you are an ACC Member when inquiring about services.

- Jordan Lawrence enables companies to establish and enforce legally defensible records policies across all media, including email. For more information, visit [www.jlacc.com](http://www.jlacc.com).

disparate information systems and technologies used at different times or by different business units within the same enterprise can make it difficult to identify routines and establish uniform standards. This challenge just got more complicated, as now you need to know which “routine operations” apply to a given ESI discovery issue and trigger the protection of Rule 37(f). The systems you need to understand might include personal computers, servers, databases, and tape backup systems, each of which may have different procedures (or routines), even within the company’s IT systems. Disputes over what constitutes a “routine” on any part of a computer network are inevitable.

### Automatic Processes

Rule 37(f) apparently contemplates affording some protection in situations where data is lost from the normal operation of automatic processes embedded in computer operating systems and applications. Every time a computer is used, including the simple acts of booting up or down (turning a machine on or off), portions of unsaved and previously deleted information in “free space” and “temporary virtual memory” on the hard drive are lost through automated

overwriting. Word processing and spreadsheet programs may also alter the integrity of ESI through dynamic applications that automatically change dates, check spelling, and adjust computations in the text of documents. The Committee Note to Rule 37(f) specifies that data loss resulting from such automatic processes is covered by the rule, stating “[t]he ‘routine operation’ of computer systems includes the alteration and overwriting of information, often without the operator’s specific direction or awareness, a feature with no direct counterpart in hard-copy documents.”

### Backup Tapes

In the event of a damage to or failure of active computer systems, most organizations maintain snapshots of ESI on backup tapes for disaster recovery. These tapes are recycled daily, weekly, or monthly, depending on the policy implemented manually by database administrators, resulting in the overwriting or loss of backup data as part of a routine. As the drafters acknowledge, “many large organizations routinely recycle hundreds of backup tapes every two or three weeks; placing a hold on the recycling of these tapes for even short periods can result in hundreds of thousands of dollars of expense.”<sup>8</sup> Nevertheless, while Rule 37(f) potentially covers data loss when executing backup tape recycling routines, the Committee Notes do not suggest continuing recycle routines in all circumstances. Similarly, if your organization has used email backup tapes for archives, and not just disaster recovery, expect to hear arguments that the ESI on those tapes is reasonably accessible, based on past performance, and is therefore discoverable.

### Databases

The drafters recognize that “[s]ophisticated and often custom-designed databases may be functional only if they continually revise the information they manage. Such information destruction features are an integral part of the computer system design and operation.”<sup>9</sup> These “routines” set up by an organization’s systems administrator on computers and backup systems to manage electronic data within a networked environment would appear to be covered under Rule 37(f), as part of the company’s necessary maintenance and regular business operations. Indeed, the Committee Note explains that the “routine operation” refers to “the ways in which such systems are generally designed, programmed, and implemented to meet the party’s technical and business needs.”

### Repurposing Hardware

IT personnel routinely use programs to “wipe” data on desktop and laptop computers before installing new

operating systems, reassigning computers to different employees, or sending old computers offsite for destruction. These processes traditionally have not had close interplay with legal compliance concerns, but these are the types of “routine operations” that may be subject to Rule 37(f). IT and HR departments will need to coordinate with the legal department when repurposing or disposing the hardware of terminated or reassigned employees to ensure that any data subject to a “litigation hold” are properly preserved.

### **Purging Emails**

To reduce the high volume and accumulation of email, some organizations use standard configurations to limit each employee’s space on servers and purge email aged beyond a certain date or that exceeds a specified size. The drafters recognized that “the regular purging of emails or other electronic communications is necessary to prevent a build-up of data that can overwhelm the most robust electronic information systems.”<sup>10</sup> A company that decides to continue the routine purging of emails after being on notice of a duty to preserve must be prepared to defend its records management and preservation policy and procedures, as well as employee behaviors that arguably could invite more cost and risk. For example, when a user exceeds the space or age limit policies applied to manage server email, it is a common practice for employees to “auto-archive” or manually “drag and drop” email in bulk into personal folders stored on the user’s hard drive or onto a shared drive. Such measures to store excess email might be sufficient to satisfy preservation obligations, but it will also result in the decentralization and over-retention of email, making it more costly to search and produce ESI, and generally increase the collateral risks of having to explain extraneous yet damaging email an employee unwittingly retained beyond its useful life.

Numerous questions remain about what is “routine” under Rule 37(f). Parties will likely seek to characterize a variety of electronic information system processes as “routine” to invoke the new rule’s apparent protections. You might argue system features that satisfy legitimate business needs, independent of any litigation, or that are integral to the system’s design or function, are “routine” purposes of Rule 37(f). Similarly, if such features are impossible or difficult to suspend or interrupt while benefiting from the legitimate, continued use of the system (or larger system of which it is part), it is reasonable to find good faith if information is lost from such “routines.”

Courts might apply similar criteria when considering arguments of undue burden or cost in respect of the reasonable accessibility of data. Whatever criteria courts use to identify a “routine operation of an electronic infor-

mation system,” if those routines can be suspended in a reasonably nonintrusive manner, the protections afforded under Rule 37(f) arguably should not apply.

Any standard of good faith implies the use of a subjective test of reasonableness, and courts will necessarily evaluate routines under Rule 37(f) on a case-by-case basis. Each organization has a different computer system architecture and varying effectiveness in the enforcement of its records management policy and procedures. Hence, the operational burdens, costs, and alternative mechanisms for data preservation will differ in every case. With this in mind:

- Be sure to communicate all computer configuration routines to the executive responsible for ediscovery and data collection, inasmuch as reliance on Rule 37(f) to excuse the continued operation of a routine still might breach the duty to preserve.
- As between legal and IT, you must have seamless communications and sound procedures to satisfy preservation duties, and identify individuals or an individual to serve as the company representative for court proceedings and depositions.
- Your management team must assess and perform a gaps analysis of the organization’s current records management policies and procedures, and specifically consider how those policies apply to ESI and so-called routines under Rule 37(f).
- Once the company has defensible policies and procedures in place, it is critical, as for any effective compliance program, that the organization appoint a high-level executive with adequate authority to oversee records management, train employees, periodically assess the program for gaps in compliance, and remediate where necessary to minimize lapses and ensure uniform implementation as best as reasonably possible.

Finally, one must empathize and keep an opponent’s potential counterarguments in mind at all times. Be prepared to respond to the argument that you have designated certain maintenance activities and customized configuration settings as routine solely to make ESI unavailable for discovery. For these reasons, among others, your corporate representative will need to be personally familiar with your records management compliance program and ready to withstand cross-examination. The question of whether sanctions apply will turn on whether a party has acted in good faith.

### **“Good Faith” Operation**

The “good faith” defense belatedly made it into the final version of Rule 37(f), and it is useful to review the rule’s history in understanding how the courts might ap-

## An Overview of the New Rules

### Rule 16: Ediscovery in the Scheduling Conference

#### Addressing Ediscovery Early

Rule 16(b) “[T]he district judge, . . . , shall, after receiving the report from the parties under Rule 26(f) or after consulting with the attorneys for the parties . . . enter a scheduling order that . . . may include . . . (5) provisions for disclosure or discovery of electronically stored information; (6) any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production[.]”

### Rule 26: The New Focus on Electronically Stored Information

#### Things Subject to Mandatory Initial Disclosure

Rule 26(a)(1)(B) “[A] party must, without awaiting a discovery request, provide to the parties . . . a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and the disclosing party may use to support its claims or defenses, unless solely for impeachment[.]”

#### Limiting Scope of Ediscovery by Identifying Reasonably Inaccessible Data Showing of Undue Burden and Expense

Rule 26(b)(2)(B) “A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If a showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.”

#### Preconference Meet and Confer to Resolve Preservation, Form and Privilege Issues

Rule 26(f) “[T]he parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties’ views and proposals concerning: . . . (3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced; (4) any 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[.]”

#### Default “Clawback” Procedure to Resolve Protected Disclosure

Rule 26(b)(5)(B) “If information is produced in discovery that

is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.”

### Rule 34: Requesting Electronically Stored Information

#### Only One Form Required, but Requestor Can Choose

Rule 34(b) “The request may specify the form or forms in which electronically stored information is to be produced . . . The response shall state . . . that inspection . . . will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection . . . If objection is made to the requested form or forms for producing electronically stored information—or if no form was specified in the request—the responding party must state the form or forms it intends to use . . . Unless the parties otherwise agree, or the court otherwise orders: (i) a party who produces the documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them with the categories in the request; (ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms that are reasonably usable; and (iii) a party need not produce the same electronically stored information in more than one form.”

### Rule 37(f): New Sanctions Shield

Rule 37(f) “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

### Other Ediscovery-Related FRCP Amendments

- Rule 33(d): Option to produce electronically stored information as business records in response to interrogatories clarified.
- Rule 34(a): Electronically stored information, stored in any medium, added to items subject to a request to produce; testing and sampling added to list of actions requestor may perform.
- Form 35: Report of Parties’ Plan Meeting updated to reflect changes to Rule 26(f).
- Rule 45: Subpoena rules updated to reflect rule changes to electronically-stored information.

ply the standard of good faith under the new rules. Early drafts did not refer to good faith but instead would have barred sanctions where the party took reasonable steps to preserve information after knowing the information was discoverable, and the data loss occurred from the routine operation of the party's electronic information system. Another version would have barred sanctions unless the party intentionally or recklessly failed to preserve the information. In both earlier versions, sanctions could apply to any data loss that violated a court preservation order.<sup>11</sup>

The prior versions of the rule approached the issue from both extremes: intentional violation of a preservation duty or simple negligence. Both were rejected. The drafters were concerned that expressly indicating that immunity from sanctions did not apply for violation of a preservation order would "create an incentive to obtain a preservation order to make the rule's protection unavailable" when the drafter believed such "orders should not be routinely entered."<sup>12</sup> They also did not believe that a "reasonableness" or negligence standard would sufficiently change the status quo (where any mistake in deciding whether to interrupt computer system operations would risk sanctions). Conversely, the drafters feared that sanctions only for intentional or reckless data loss would have invited "discovery and fact-finding that could involve inquiry into difficult subjective issues" as well as "insulate conduct that should be subject to sanctions."<sup>13</sup>

To resolve these concerns about the earlier versions of Rule 37(f), the drafters ultimately adopted the good faith standard to measure culpability on a case-by-case basis. Only time and practice will teach whether using a good faith standard will encourage motion practice and incite the "discovery on discovery" phenomenon the advisory committee sought to avoid.

As noted, the new rules are procedural and thus do not prescribe the scope or timing of the duty to preserve. As the advisory committee notes, "[t]he rule itself does not purport to create or affect such preservation obligations, but recognizes that they may arise from many sources, including common law, statutes, and regulations."<sup>14</sup> Thus, a party may be exposed to sanctions for allowing information subject to a preservation duty "to be destroyed in order to make it unavailable in discovery by exploiting the routine operation of an information system."<sup>15</sup> Without prescriptive guidance in the new rules, your law organization will regularly face difficult decisions about whether to "intervene to modify or suspend certain features of the routine operation of a computer system to prevent the loss of information, if that information is subject to a preservation obligation."<sup>16</sup>

If your organization is unable to produce ESI sought in

discovery and wants to rely on Rule 37(f) for protection from sanctions, prepare to carry the burden of showing your company acted in good faith. The Committee Note advises that "[a]mong the factors the bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information." In other words, prepare to produce contemporaneous documentation to explain the steps taken to ensure thorough and complete compliance with preservation obligations, by minimizing communication lapses, human error, and inadvertent destruction of data. For companies who lack effective record retention policies and procedures, it will be most difficult to show good faith, inasmuch as one cannot argue having routines without standards in the first place.

The organization could argue that suspending the process that resulted in the loss of ESI would have caused undue burden and cost by producing an "even greater accumulation of duplicative and irrelevant data that must be reviewed, making discovery more expensive and time-consuming."<sup>17</sup> This argument can easily backfire, however, if, for instance, the company did not suspend a configuration that deletes emails over a specific size limit or outside a set date range. If the email lost were subject to a preservation duty, it is hard to fathom a court finding that the ESI was lost due to the good faith, routine operation of the system.

Demonstrating good faith will be a slippery and treacherous slope for organizations where routines are merely a paper goal, rather than actual practice. Litigants may have difficulty providing any plausible explanation, let alone showing good faith, after litigation has commenced, if:

- ESI is purged by the recycling of backup tapes that the organization has in the past accessed to extract ESI for business or legal reasons; or
- ESI is deleted from a laptop or hard drive because the employee never received actual or constructive notice of circumstances giving rise to a duty to preserve, due to a records management compliance program lacking adequate education and awareness.

If required to demonstrate good faith, a party will need to produce documents showing the scope, methods, and reasons for steps taken—and not taken—in the preservation and discovery process. An effective records and information management program will facilitate better internal communication and go a long way toward showing good faith. No policy is foolproof, but a records management policy that is communicated and well understood across the organization and periodically audited should pass muster under a standard of good faith.

## Inaccessible Data and the New Sanctions Shield

There is a tension between the implied duties to preserve under Rule 37(f) and the ability to withhold production of inaccessible data under the new procedures outlined in the amendment to Rule 26(b)(2). Under this amended rule, a party may decline to search and produce ESI that are not reasonably accessible due to cost or burden. Purported inaccessibility, however, does not obviate the need to retain the information. Indeed, the Committee Note makes clear that good faith may require preservation of information from inaccessible sources. Simply put, the duty to preserve is broader than the duty to produce, and the failure to preserve inaccessible data, even due to routine operations of an information system, may result in Rule 37 sanctions.

For example, if you tell your adversary that you will not search monthly backup tapes retained from the past several years for responsive information on the ground of inaccessibility, and these tapes are subsequently recycled, the court may still assess sanctions if it finds the organization breached its duty to preserve the data on these tapes. The fact that data is inaccessible, therefore, does not preclude a court from ordering discovery for good cause or even under a cost-shifting formula.

There is no bright-line rule to measure when a party has discharged the duty to preserve. The Committee Note acknowledges as much, stating that the answer “depends on the circumstances of each case. One 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.” Ironically, if a party classifies certain ESI as inaccessible in discovery proceedings and fails to preserve the information, it may undermine a showing of good faith if the ESI is subsequently lost, causing more prejudice to their legal position than if the party had never identified the loss of data at all. With the latter, a party may be able to show entire lack of awareness of the data or its potential relevance, whereas with the former, a party will have to show why identified data was lost.

Rule 37(f) highlights the significant burdens that preservation of ESI, particularly from inaccessible sources, may place on an organization. The new requirement to identify sources of inaccessible data, which in the past were generally ignored,<sup>18</sup> may in practice lead to excessively broad preservation demands. The Committee Note to Rule 26(f) tries to head off that impulse by exhorting parties to “pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities.” This note cautions that “[c]omplete or broad cessation of a party’s routine computer operations could paralyze the party’s activities,” and

therefore “[t]he parties should take account of these considerations in their discussion, with the goal of agreeing on reasonable preservation steps.” Parties who receive preservation demands from an adversary may find this exhortation a useful reference to re-focus the discussions. Even before the rule became effective, a court relied on this rationale to criticize a plaintiff’s pre-suit demand that the defendant “for an indefinite time not modify or delete any electronic data in any mainframe, desktop, or laptop computers, or other storage media or devices, and not upgrade or replace any equipment or software.”<sup>19</sup> The court noted that such a preservation demand failed to “accommodate the routine day-to-day needs of a business with a complex computer network,” and indicated that “Rule 37(f) recognizes that discovery should not prevent continued routine operation of computer systems.”<sup>20</sup>

If a party plans to invoke a Rule 37(f) defense, it had better be sure the organization’s routines for handling ESI can withstand scrutiny. Otherwise, misplaced use of this defense could invite unwanted examination of an organization’s IT processes, compliance systems, and records management policies, and possibly expose problems that bring into question the completeness of the data production in the pending case as well as other matters. In 2006, the SEC sanctioned Morgan Stanley & Co., Inc., for example, for failing to produce email and not diligently searching for backup tapes containing responsive email after state court civil litigation revealed electronic discovery deficiencies. Details are available at [www.sec.gov/litigation/litreleases/2006/lr19693.htm](http://www.sec.gov/litigation/litreleases/2006/lr19693.htm).

## Murky Waters: Exceptional Circumstances and Other Sanctions

Notwithstanding the good faith of the parties, Rule 37(f) gives courts leeway to fashion equitable remedies and impose sanctions in “exceptional circumstances.” The advisory committee report notes that the exceptional circumstances provision “adds flexibility” and “permits sanctions . . . even when information is lost because of a party’s good-faith routine operation of a computer system.”<sup>21</sup> As to what may constitute exceptional circumstances, the following example is provided: “an *entirely innocent party* requesting discovery against *serious prejudice* arising from the loss of *potentially important* information.”<sup>22</sup> To the extent the sanctions defense of Rule 37(f) is intended to reduce the amount of discovery motion practice over electronic discovery, courts should judiciously invoke the “exceptional circumstances” remedy or risk eroding any benefit from the amendment.

If all this has not dampened one’s spirit enough, consider that Rule 37(f) only bars imposition of sanctions “under these rules,” a limitation that leaves available possible grounds for sanctions arising from statute, the inherent power of the

court, or professional ethics rules. Nevertheless, if a party seeks protection under Rule 37(f), and has made good faith efforts to implement and sustain effective records management practices, as a matter of public policy, it is difficult to see a circumstance where the court would still reach into its inherent power to impose harsh sanctions. As the Committee Note indicates, short of sanctions, a court may make adjustments in how discovery is managed if a party is unable to provide relevant responsive information. We might see, for example, a court use Rule 37 to order additional depositions, interrogatories, or that the non-moving party “provide substitutes or alternatives for some or all of the lost information.”

### Batten Down Your Hatches

The new amendments require you and your outside counsel to know about the electronic data generated and stored on company computer systems earlier and much more intently than ever before. The parties need to come to scheduling conferences prepared with detailed and complete data preservation plans, including clear explanations regarding inaccessible data, and a plan for searching and producing responsive data. Questions about preservation have engendered considerable uncertainty “as to whether a party must, at risk of severe sanctions, interrupt the operation of the electronic information systems it is using to avoid any loss of information because of the possibility that the information might be sought in discovery.”<sup>23</sup> New Rule 37(f) presents the lure of a sanctions shield and may tempt companies to continue routine operations of their IT systems or adopt new ones in the hopes of immunizing themselves from sanctions. While tantalizing, however, the good faith and other eligibility requirements for application of Rule 37(f), as well as the open questions about its scope, should make reliance on this shield a risky proposition. ❏

Have a comment on this article? Email [editorinchief@acc.com](mailto:editorinchief@acc.com).

#### NOTES

1. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, No. CA 03-5044 AI, Order on CPH’S Renewed Motion for Entry of Default Judgment (Fla. Cir. Ct., 15th Judicial Circuit, Palm Beach Cty, Mar. 23, 2005) (Morgan Stanley’s poor controls for handling email archives led to adverse inference jury instructions and contributed to a \$1.45 billion judgment against Morgan Stanley) (**APPEAL PENDING?**); *Thomson v. U.S. Dep’t of Housing and Urban Dev.*, 219 F.R.D. 93, 104 (D. Md.2003) (belated production of 80,000 emails after discovery cutoff deadline warranted sanctions, including precluding defendants from use of emails at trial); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 439 (S.D.N.Y. 2004) (sanctions imposed for producing relevant emails two years after discovery request and destroying others after on notice of duty to preserve). Likewise, the SEC, self-regulatory organizations, and other regulators have fined companies for failure to produce electronically stored informa-

- tion, most notably in the financial services industry (e.g., in 2006, SEC assessed \$15 million fine against Morgan Stanley and \$2.5 million against Merrill Lynch for failing to produce emails promptly).
2. See Report of the Judicial Conference Committee on Rules of Practice and Procedure to the Chief Justice of the United States and Members of the Judicial Conference of the United States, September 2005 [hereafter “Judicial Conference Committee Report”] at p. 23.
  3. *Zubulake V*, 229 F.R.D. at 441.
  4. The Judicial Conference’s Advisory Committee on Evidence Rules has proposed adding Rule 502 to the Federal Rules of Evidence, which, if codified into law, would protect parties from waiving attorney-client and work product privileges in limited circumstances, including use of the new procedures set forth in Rule 26(b)(5)(B) of the Federal Rules of Civil Procedure. The Advisory Committee on Evidence Rules is hearing public comments on proposed Rule 502 through February 15, 2007. Following the public comment period, and any approved changes, proposed Evidence Rule 502 will require an affirmative act of Congress, and will take effect on December 1, 2008, unless altered by Congress.
  5. Substantive questions of waiver of attorney-client privilege and work product will arise more frequently under the new rules in the context of ESI, and may be addressed in part through proposed adoption of Rule 502 of the Federal Rules of Evidence and a codified doctrine of inadvertent waiver; however, consideration of those issues are beyond the scope of this article.
  6. *Thompson v. U.S. Dep’t of Housing and Urban Development*, 219 F.R.D. at 98–99 (courts can require parties “to identify experts to assist in structuring a search for existing and deleted electronic data and retain such an expert on behalf of the court”).
  7. No such defense from sanctions for the unavailability of paper records is provided because paper “is not destroyed without an affirmative, conscious effort. By contrast, computer systems lose, alter, or destroy information as part of routine operations....” Judicial Conference Committee Report at 32.
  8. See Judicial Conference Committee Report at 33.
  9. *Id.* at 34.
  10. *Id.* at 33.
  11. Report of the Civil Rules Advisory Committee, To Hon. David F. Levi, Chair, Standing Committee on Rules of Practice and Procedure, May 27, 2005 (Revised July 25, 2005) [“Advisory Committee Report”] at 87–88.
  12. *Id.* at 83.
  13. *Id.* at 82.
  14. *Id.* at 83.
  15. Judicial Conference Committee Report at 34.
  16. *Id.* at 34.
  17. Advisory Committee Report at 81.
  18. See Judicial Conference Report at 31 (citing the new rule as an improvement over old-rule practice, “in which responding parties simply do not produce electronically stored information that is difficult to access”).
  19. *Turner v. Resort Condominiums International, LLC*, 2006 U.S. Dist. LEXIS 48561, \*16 (S.D. Ind. July 13, 2006).
  20. *Id.*
  21. Advisory Committee Report at 83.
  22. *Id.* at 86 [emphasis added].
  23. Judicial Conference Committee Report at 33.