



NOVEMBER 13, 2006

# Finding a **Safe** Harbor

*Before relying on sanctions shield in electronic discovery, companies need to get their IT house in order.*

BY **BERYL A. HOWELL**  
AND **RICHARD J. WOLF**

**L**EGAL RISKS from underdeveloped electronic discovery processes are escalating rapidly and forcing organizations to bring order to the explosion of sprawling and decentralized information technology and telecommunication systems. Though not all organizations have experienced e-discovery and its high costs, the exposure will become commonplace for almost every litigation when new amendments to the Federal Rules of Civil Procedure relating to “electronically stored information” (ESI) become effective next month.

While compliance with legal preservation obligations has tradition-

ally been part of the in-house counsel portfolio, that paradigm is changing. A new governance model is emerging to charge the IT, audit, legal and compliance functions with shared responsibility for crafting, implementing, training, and auditing compliance with data retention policies, and providing reliable, verifiable information to outside counsel for use in court about the management of ESI.

Companies will need to be able to answer regularly in court questions about the full life cycle of data, with questions ranging from when data was created or received and on which media, all the way through storage and ultimate disposition. Outside counsel will need timely assistance to satisfy the new rules’ requirements for early identification of data subject to discovery.

A greatly anticipated aspect of the new amendments is a sanctions shield in the proposed amendment to Rule 37(f), which could bar the imposition of penalties when a party is unable to provide ESI “as a result of the routine, good-faith operation of an electronic information system.” The proposed rule does not relieve a party from

any preservation duty or the new requirement to identify information sources that “are not reasonably accessible because of undue burden or cost.” Yet, many organizations do not have effective policies or a firm grasp on their current or legacy systems used for e-mail and other types of data they generate or receive, sometimes across multiple business units that span the globe. Thus, compliance and legal professionals may look to use proposed Rule 37(f) as an internal cudgel to bring order and enforcement to records management policies and procedures.

## **IT Housekeeping**

Before relying on Rule 37(f), organizations should have their IT house in sufficient order to be able to identify and verify compliance with information system “routines,” and any exceptions that arise due to litigation holds. This exercise will provide the added benefit of giving organizations a head start on being able to identify early in litigation data that are not reasonably accessible and exempt from the scope of searching for responsive information, absent

**Beryl A. Howell** is a partner of Stroz Friedberg LLC, a technical services and consulting firm, and a commissioner on the U.S. Sentencing Commission. **Richard J. Wolf** is president of the Greater New York Chapter of the Association of Corporate Counsel and managing partner of Lexakos Consulting LLC, an advisory group.

agreement of counsel or a court order.

Companies will need to know which “routine operations” will fall under the protection of proposed Rule 37(f). Electronic information systems are comprised of workstation computers, servers, databases and backup systems, each of which may be subject to different “routines.” The new rule apparently contemplates some protection for data lost from automatic processes embedded in computer operating systems and applications, such as word processing programs that automatically update or even erase certain data upon boot-up or shut-down of a computer. Similarly, “routines” set up by an organization’s systems administrator for servers and backup systems to manage ESI within a networked environment would appear to be covered under proposed Rule 37(f), insofar as they are part of the company’s necessary maintenance and regular business operations.

Information system practices vary in the degree of manual input and automation, and there are real space, time and cost implications, as well as risks, associated with implementing new, or stopping regular, IT procedures. How courts will evaluate these varying factors to decide whether a particular IT practice is a “routine” is an open question. At a minimum, organizations should not consider reliance on proposed Rule 37(f) to seek forgiveness for data lost due to a routine’s continued operation in the face of a preservation duty.

### **Records Management Policy**

Courts will need to evaluate routines on a case-by-case basis, because every organization has different network system architecture

and data management procedures. Companies need to take a close look at the effectiveness of current records management policies and how those rules apply to ESI, if at all, and identify practices that could be construed as “routine” under the proposed Rule 37(f).

### **An effective records and information management policy will help show good faith.**

The loss of ESI sought in discovery may only be excused by a good faith showing. Demonstrating good faith in the operation of a routine could end up being a slippery and dangerous slope for organizations where routines are merely a paper goal, rather than actual practice. To demonstrate good faith, a party may have to explain the scope, methods and reasons for a particular routine and for the steps taken—and not taken—in the preservation and discovery process. An effective records and information management policy will facilitate internal communication, effective hold management and help show good faith. No policy is foolproof. But a records management policy that is communicated well across the organization and periodically audited should pass muster under a standard of good faith.

Proposed Rule 37(f) may provide an incentive for organizations to have a centralized records management policy, with uniform enforcement practices across business lines. In this way, the organization can provide consistent answers about

its “routines,” retention policy compliance practices, and the relative costs and burdens of accessing ESI.

Organizations in the process of getting ready for the new rules should consider: (1) assessing current IT policies and actual “routines” on handling ESI; (2) identifying the location of relevant data by performing a high-level inventory of servers, backup tapes, portable storage devices and hard drives; (3) evaluating and, if necessary, reengineering processes for communicating litigation holds to suspend routines that may affect data subject to preservation obligations; (4) crafting a preservation process plan that specifies relevant data to be preserved and methods to safeguard the information from corruption or destruction; (5) establishing regularly scheduled audits to monitor compliance with records management policies and litigation holds; and (6) establishing a centralized records and information management corporate function with a cross-functional e-discovery team that coordinates and enforces all these activities.

The lure of a sanctions shield in proposed Rule 37(f), as well as the other new rules’ requirements, should encourage organizations to improve not only the management of their electronic data but also the knowledge management about their internal systems.

---

This article is reprinted with permission from the November 13, 2006 edition of the GC NEW YORK. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit [www.almreprints.com](http://www.almreprints.com). #099-11-06-0002