Electronic Data Discovery and the New Federal Rules
More Risks To Be Addressed By Compliance and Ethics Programs

By
Christopher A. Myers
And
William F. Hamilton
Holland & Knight LLP

Introduction

On December 1, 2006, significant changes to the Federal Rules of Civil Procedure (FRCP) specifically directed to discovery of electronic data (E-Discovery) went into effect. The rules were amended to provide guidance and mandatory direction necessitated by the explosion of electronically stored information (ESI) in the past several years. The amendments, read in their totality, express underlying principles which mandate new practices. Among the most important of these are: (1) early ESI self-examination; (2) prompt and thorough ESI preservation decisions; and (3) early, open and frank discussions with the opposition on both the preservation and production of ESI. Without significant attention to these new requirements, including the development and implementation of comprehensive records management programs and their integration into the framework of an effective compliance and ethics program, litigants and the subjects of government attention face onerous expenses and costs, draconian sanctions and litigation or investigation failures.

The New E-Discovery Rules

The FRCP definition of "relevant information" is extremely broad. It includes all documents "reasonably calculated to lead to the discovery of admissible evidence." Given the almost unthinkable volume of ESI in today's business world and the volatility of ESI , corporate counsel (and compliance officials) are now under tremendous pressure to quickly issue preservation orders of the appropriate scope and then determine what components of ESI will be searched for potentially relevant data. Further, counsel must also determine how to accomplish such searches, and then review and produce responsive data, with maximum efficiency and minimum expense. Counsel is now required under the new Amendments to make a series of nearly immediate judgment calls that may subsequently be questioned by the courts and opposing counsel. Worse, because of the transitory nature of electronic documents, there is likely no chance for a "do-over" if a judgment call is later questioned. For example, what if a back-up tape or other ESI storage media located at a geographically remote subsidiary is not preserved, but two years into the litigation it turns out that the former human relations manager's reports are now relevant, because that former human relations manager is now a division head at a sister corporation. Will the company be subject to sanctions? Will the court issue adverse inference instructions to the jury?

To make matters worse, in the context of government investigations, such as under the False Claims Act, or the securities laws, will the Department of Justice, or SEC investigate the company *and* its officials, for Obstruction of Justice, or False Statements violations based on the

failure to preserve records, or inaccurate statements regarding the existence of certain records. Or, will law enforcement agencies and prosecutors impose their own version of an adverse inference by concluding, based on the failure to preserve records, that the scienter, or intent element of the charges they are investigating, is supported by this failure.

The risk of future untoward consequences such as sanctions and adverse inferences can be minimized by following the procedures contemplated in the Federal Rules Amendments, and by incorporating them into a comprehensive records management program. We strongly recommend that the records management program come first. For reasons which will become clear, however, we will discuss the procedures under the Amendments first, because they illustrate the need for the records management program. It is further our strong recommendation, that records management programs come under the umbrella of a comprehensive compliance and ethics program.

The three key procedures under the Amendments are as follows. *First*, as soon as the litigation or investigation begins, or as soon as the duty to preserve records is otherwise triggered, conduct a thorough ESI self-analysis. *Second*, based on the ESI self-analysis, make prompt preservation decisions, communicate those decisions to all necessary individuals, and make sure those decisions are properly implemented. *Third*, analyze the cost and expense of both your document preservation and the required search of your ESI locations for relevant data. Promptly schedule the Rule 26(f) conference (or a meeting with government investigators) and disclose your analysis and decisions. If the opposing side agrees, you will have a strong response if ESI evidence has been lost or can only be recovered at great expense. If the opposing side does not agree with your preservation, search and production decisions, you have an early opportunity to seek guidance from the court, or to negotiate a common understanding with the government investigators.

Step 1: The Initial Self-Analysis

When litigation or an investigation are "reasonably anticipated," a duty to preserve potentially relevant records, including electronic records, is triggered. It is very easy to underestimate the scope of the documents the opposition, or the government, will request and which may be relevant to claims or defenses in the case. A good exercise is to assign one member of the attorney team to step into the role of the other side in the matter, and assign him or her the task of developing a list of categories of all documents the other side may request, or which might be relevant. One good practice is to list every potential issue in the case and then identify every potential custodian that may have touched documents relevant to that issue. This is not a simple exercise. Depending on available resources, this task should be attacked by a team, at minimum, composed of a lawyer and employees at the core of the matter. Also, be careful not to confuse "custodians" with "witnesses." A secretary may be a likely custodian, but not a likely witness.

Next, the IT department must be involved. The possible locations for ESI for each custodian must be considered and documents. They may include: laptops, servers, Blackberries, home computers, network file servers, Exchange, or other email servers, flash drives, discs in drawers, back-up tapes, etc. The IT department's active cooperation is crucial for an understanding,

search and preservation of these various sources. Each custodian must also be questioned regarding possible locations of ESI (as well as traditional paper documents).

Step 2: The Initial Preservation Decisions

The next step is both critical and difficult. What data of each custodian must be promptly preserved and by what method. First, a few basic rules: the hard drives of all core witnesses and custodians should be immediately preserved bit by bit. This requires making a "mirror image" of these hard drives. That will capture all of the "active" data on the drive, plus the deleted matter that has not been written over. Don't forget the email and file servers. Make sure to take a full snapshot of the server, which essentially takes a picture of all documents on the server and will prevent the inadvertent loss of any relevant data. Issue litigation, or document destruction "holds" to all custodians and make sure that the IT department suspends any automatic delete functions of the system. In addition, all back-up tapes that have captured data from the core custodians should be preserved. At a minimum, a temporary hold should be placed on the rotation of back-up tapes that may have captured relevant data.

The next question is, how much data beyond the core custodians must be preserved. This decision can be complex and depends on several factors, including the potential value of the case, the locations of the data, the number of custodians, the potential relevance of any Metadata to the case, and, of course, the cost of preservation and retrieval. The key issue here in minimizing potential sanctions is to document your decisions. The risk of sanctions, criminal charges and other horribles is dramatically reduced if your decisions are based on an informed, reasonable assessment of the value, or potential value of the data and the expense of preservation and production. As will be seen, if these decisions are made pursuant to a carefully designed records management program that has been implemented in good faith, and which are documented in a way that can be followed by the opposing party and the court, the basis for sanctions will be difficult to establish. The compliance and ethics officer and staff can help with this process and with the periodic follow-up which will be required. This will be discussed in more detail below.

3. The Rule 26(f) Meeting and Disclosures

The biggest safety net for a company and its counsel in this complex process is the Rule 26(f) conference. The conference is the principle disclosure point, and through disclosure comes the maximum protection and risk reduction.

The Rule 26(f) conference must be the subject of thorough preparation. At a minimum, counsel must be prepared to discuss the following E-Discovery topics:

1. All locations of ESI, (including back-up tapes);
2. The kinds of ESI (emails, spreadsheets, digital voice, etc.);
3. The accessibility of ESI;
4. The cost of retrieving ESI;
5. The methods and searches for retrieving ESI;
6. The materiality and relevance of the various locations of ESI;
7. What ESI should be preserved in its original form;

8. The costs of preservation of ESI (the cost of forensic images and back-up tapes);
9. The form of ESI production.

The Rule 26(f) conference should be undertaken as early as possible in the litigation. Why? Because these disclosures and procedures provide the company and its counsel with a safety net. If the opposition accepts proposals and decisions regarding ESI, then the potential for future sanctions related to deleted, lost or otherwise destroyed information is dramatically reduced, if not eliminated. On the other hand, if the opposition does not agree with your decisions, they can be modified promptly, sometimes at the cost of the opposition. In addition, early discussion gives you the opportunity to take disagreements to the court.

This is also true in the context of a government investigation. Although there is no Rule 26(f) conference in a criminal or civil fraud investigation, if preservation decisions and parameters are proposed to and agreed to by the government investigating agency, or the Department of Justice, it would be difficult for them to later argue that you have obstructed the investigation. It is particularly important in criminal cases to document any agreements with the government on this issue. Sometimes investigations can continue over a period of years. Lead prosecutors and agents frequently change. Without good documentation, it can be difficult to confirm, or provide evidence of preservation agreements that happen at the beginning of an investigation.

The Importance of a Comprehensive Records Management Program

As can be seen from the recommendations above, companies must be in a position to take action virtually immediately once they have reasonable anticipation of litigation or investigation. The initial self-analysis and the preservation decisions must be undertaken quickly and efficiently. Employees must receive guidance, and procedures need to be in place for establishing, enforcing and documenting the litigation hold activities. In order to prepare for and attend the Rule 26(f) conference, or to meet with prosecutors or regulatory agents in a criminal or civil investigation, you need to quickly analyze and propose preservation and production parameters. You need to be in a position to present and argue cost issues to protect your client from potentially massive discovery costs, potential sanctions, and, in the criminal context, from Obstruction of Justice and False Statements liability.

The best way to accomplish all of these things in an efficient, cost effective manner is to have a fully implemented, comprehensive records management program in place. Such a program would have a written set of policies and procedures tailored to the business methods of your company. These procedures would then be integrated into operations; employees would be trained; the procedures would be enforced and compliance monitored and audited. It would be incorporated into the company's culture, and there would be communications from senior management about its importance.

Good records management programs can save companies hundreds of thousands of dollars, possibly more. They establish processes to keep records that the company needs or is required to maintain and to destroy documents the company no longer needs. In today's more and more electronic world, reduction of records storage costs can be a tremendous benefit to the bottom line. Thus, for example, many companies are choosing to delete, or overwrite emails that are

more than thirty days old. This can be an appropriate cost saving decision. As another example, consider backup tapes, which were created to allow the restoration of operations after a catastrophic failure. Many companies are now evaluating the need to retain back-up tapes for periods beyond reasonable usefulness. Because the current incredibly low cost of storing electronic data often fails to trigger an IT budgetary review, some companies awake after years of slumber to find themselves burdened with terabytes of data, worthless for any business purpose. However, what was perceived as a minor IT budget item may become a massive litigation expense if the stored data must be restored, processed, and reviewed. Failure to confront data storage results in a de facto decision to keep the data. And this de facto default decision is often the wrong decision. Equally important, in light of the sanctions that are possible for failure to preserve documents that might be relevant to litigation or investigations, your company must be able react promptly to possible lawsuits or investigations and to stop any destruction of relevant records. The records management program should contain procedures for accomplishing this as well.

The Role of the Compliance and Ethics Program

All of these complex analyses, decisions and implementation decisions should not simply be left to the IT Department, as is currently the case in many companies. These activities are best accomplished in the context of a company's compliance and ethics program. The compliance and ethics program should include records management, retention and preservation issues in its annual risk assessment. The compliance officer and his or her team should meet with representatives of the various legal, operational and management departments to discuss and help in the process of devising a records management system which will work in the context of the organization's size and business activities. In light of the risks of a compliance breakdown, records management should be one of the priorities of the compliance and ethics program until a functioning system is in place.

The compliance department, whether it is independent, part of the legal department, part of a risk management department, or is organized in some other way, is in the best position to understand the processes needed to implement a records management program and integrate it into the organization's operations. These requirements follow the elements of an effective compliance and ethics program, and include: risk assessments; written standards; designated compliance personnel; training and communication, auditing and monitoring; incentives and discipline; remedial action and periodic revisions. Compliance professionals understand these elements and can help make them work effectively in the context of a records management system. The compliance team should collaborate closely with the legal team and the business personnel to address this new, and growing compliance risk area.

Conclusion

E-Discovery and the new rules that govern it present the specter of formidable costs and significantly increased litigation and investigation risks. But, both the costs and risks of E-Discovery can be dramatically reduced through a comprehensive records management program

combined with the hard work of self-analysis, reasoned preservation of relevant records; and appropriate disclosure, either under Rule26(f) or in the context of an investigation.

Christopher Myers can be contacted at chris.myers@hklaw.com. William Hamilton can be contacted at william.hamilton@hklaw.com