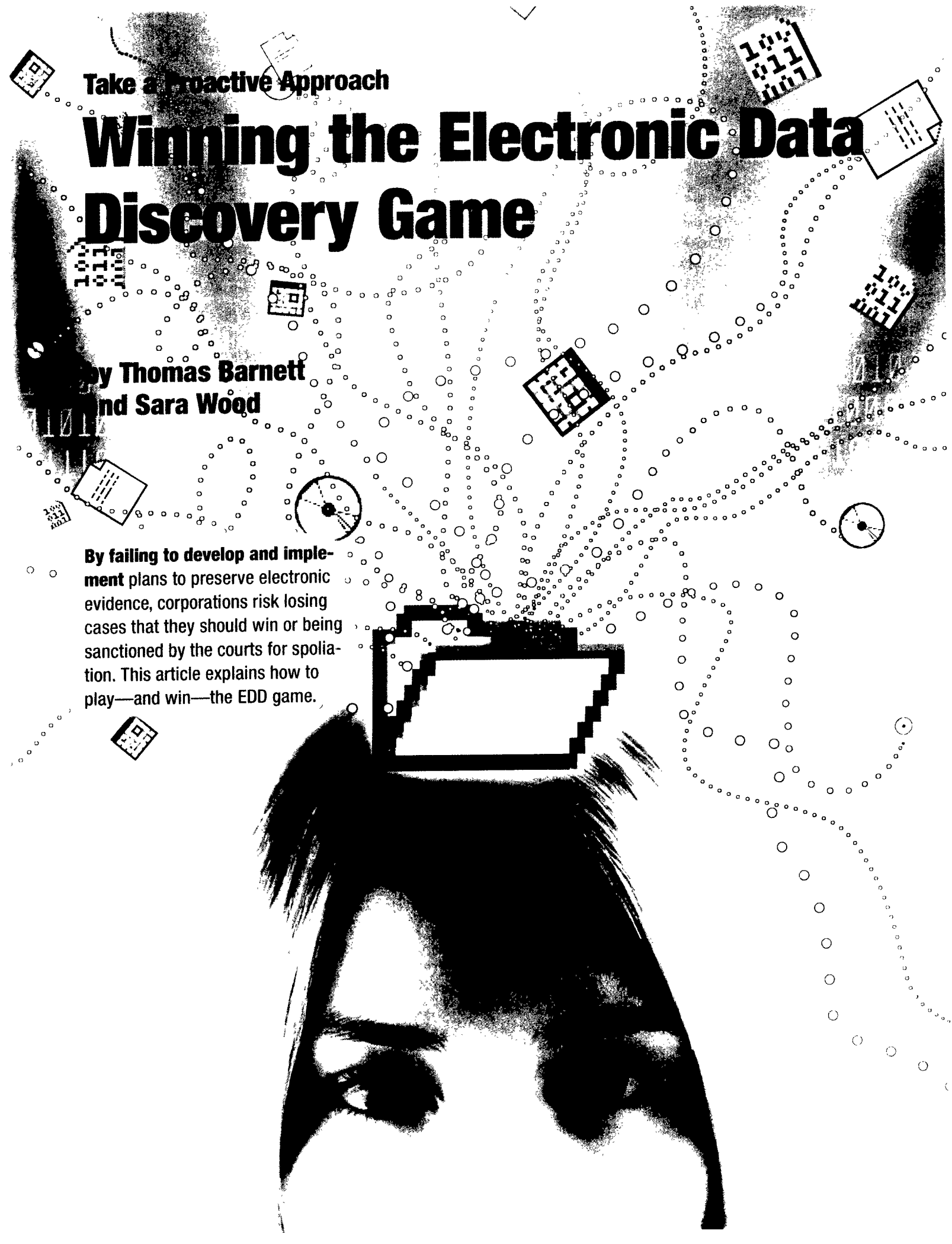
Take a Proactive Approach

Winning the Electronic Data Discovery Game

by Thomas Barnett
and Sara Wood



By failing to develop and implement plans to preserve electronic evidence, corporations risk losing cases that they should win or being sanctioned by the courts for spoliation. This article explains how to play—and win—the EDD game.

Electronic data discovery is giving plaintiffs' lawyers a powerful weapon with which to attack corporations—and many corporations aren't prepared to fight back. Without adequate preparation, they could be sitting ducks.

It is a fact of life that discovery of electronic information has become a focal point for corporate litigation and regulatory enforcement actions. The SEC and the NYSE are reported to have a number of e-mail retention cases in the pipeline and recent rulings in civil actions indicate that the stakes are getting higher for non-compliance.

A savvy plaintiff's lawyer aware of the current legal and regulatory climate can create an enormous burden on a corporation by seeking, *ex parte*, a sweeping order for a company to preserve all of its electronic data. Not only might such a preservation order strike defense lawyers as outrageously unfair, it presents a nearly impossible task, and mounting an effective response is difficult if the company is ill-prepared. Without a sound policy for electronic document retention and preservation for litigation, the company risks allowing a plausible argument to be made that it could be destroying relevant documents without realizing it. The mere prospect of having to preserve everything, generating costs into millions of dollars per month, can pressure a corporation to settle a lawsuit on unfavorable terms, or at a minimum, can affect the strategy for managing the litigation.

Electronic data discovery has also given plaintiff's lawyers a new favorite word: "spoliation." If a company is routinely destroying documents, paper or electronic—even as a routine part of its data management policy—a plaintiff's lawyer need only locate a single electronic copy of a relevant document that was not produced in order to lodge a claim of spoliation, however spurious it may be. Similarly, a paper printout of an e-mail can raise the question: where's the electronic version? A large company might have several hundred million, or even billions, of electronic documents or e-mail messages stored on servers, backup tapes, hard drives, CDs and other devices in hundreds of locations.

How vulnerable are U.S. corporations? In 2003, Cohasset Associates asked some 2,200 records management professionals about inclusion of electronic records in their organization's retention schedule. They discovered that almost half of these organizations (47 percent) did not include electronic records in their retention schedules.

According to another nationwide survey, corporate attention to e-mail and instant messages is even lower. A survey of 840 U.S. companies taken in 2004 by the American Management Association and The e-Policy Institute found that only 35 percent have an e-mail retention policy in place and that just six percent retain instant messages. The same survey found that more than one in five employers (21 percent) have had employee e-mail and instant messages subpoenaed in the course of a lawsuit or regulatory investigation.

Common sense would suggest that once litigation is underway or anticipated, companies would take reasonable steps towards the preservation of relevant electronic records to ensure their availability for discovery—not to mention the need to adequately assess the merits and defenses of the case by defense counsel. Yet, according to the Cohasset survey, 65 percent of organizations do not include electronic records in their litigation record holds. It is worth noting that a lot of attention has been focused on these issues since the passage of the Sarbanes-Oxley corporate fraud and accountability law and these numbers have likely improved.

Nevertheless, it appears that a surprisingly significant number of corporations view such disregard for electronic evidence as a minor oversight. Unfortunately for them, the courts are not so forgiving. A series of court decisions, including a significant decision in the Second Circuit, *Zubulake v. UBS Warburg*, have made it clear that corporations faced with litigation have a duty to preserve electronic evidence starting from the time the litigation is anticipated. Companies claiming that electronic data was lost or destroyed unintentionally are frequently getting a deaf ear from the courts. The bottom line is clear: develop an effective policy for preserving electronic data now or face the risk of sanctions later.

Caught in the middle are the corporate lawyers, the company's outside counsel and others deemed to have primary responsibility for preserving relevant documents during litigation. Even the company's information technology staff can be sanctioned if the court thinks they failed in their responsibilities—and in many corporations, IT staff see document retention for litigation as well down on their list of priorities. Outside counsel, EDD experts and vendors are also not immune to potential sanctions and public retribution, as recent rulings illustrate.

Even where a corporation recognizes the issues and risks, many corporate legal departments do not have enough resources to plan and implement an effective document retention policy, let alone electronic data litigation hold and data preservation processes and procedures. Nor are IT departments likely to come up with the personnel or funding.

Win C-Level Support

For in-house counsel facing the challenge of getting their companies in compliance with discovery mandates, this article suggests a number of proactive steps. The first step is to garner the support of senior

Thomas Barnett is Special Counsel at the firm of Sullivan & Cromwell LLP in New York City. Sara Wood is a Project Manager at SPI Litigation Direct in New York City.

management, especially the CEO and, if possible, the board of directors. Such support can guarantee the necessary financing and bring all affected parties into line behind the new policy.

Persuading management of the need to develop a sound e-document retention and preservation policy should not be difficult. Getting funding approved is another matter. But the case for diligence and caution is clear and the headlines are filled with disaster stories of companies that failed to take appropriate precautions. If the company loses a major lawsuit or pays out millions in fines because of sanctions for spoliation, shareholders and the market will inevitably look to senior management for accountability and take it out on the stock price. The incentives and the risks are evident.

Develop a Retention Plan

Most corporate lawyers are neither technology nor records management experts. Therefore, the most effective way to develop defensible data preservation and retention plans and procedures is to assemble a team using internal and, if necessary, external resources with appropriate expertise and familiarity with the company's records and computer systems. The team should include representatives from information technology and security, records management, and legal, as well as the departments that will be responsible for implementing and enforcing the policies. Such groups may include human resources, accounting and finance, or sales.

Because preserving and collecting electronic data for litigation has not been a standard part of the IT department's foundation, it is important for IT professionals to understand that their participation is crucial to the success of the project. Without buy-in and active participation from IT professionals within the corporation, any program to manage electronic data for litigation or records retention purposes will likely be doomed to fail.

Nevertheless, it is important to realize that IT departments have limited resources to carry out their basic mandate—keeping the corporation's data systems running and secure. When counsel directs an IT department to radically alter its processes to preserve additional data, the added burden will require additional human resources, as well as media and storage costs that can easily exhaust the IT department's budget. The legal department, outside counsel and EDD or records retention experts must therefore strive to define a reasonable process that targets the preservation of potentially relevant data without sweeping in everything under the sun.

It is important for IT professionals to understand that their participation is crucial.

Assess and Map

A key first step in developing a retention plan is to assess what data is likely to be relevant for the types of litigation the company typically faces and where it's kept. This may sound like a simple matter, but unfortunately it is not. In a large company relevant data is likely to be stored in many places: individual employees' hard drives, network file and e-mail servers, and in document management systems and company-wide software applications such as those used for human resources and accounting. Still more data can often be found on media such as CDs, DVDs and the bevy of ever-shrinking portable storage devices such as thumb drives—not to mention home computers, PDAs—the list goes on and on.

A thorough plan must also consider how the data of departing and former employees is handled. At many companies, when departing employees turn in their laptops, the laptop disk is wiped and the unit is given to another employee. A reasonable approach to avoiding destroying potentially relevant data could specify that such data not be wiped until the employee (and if necessary, their computer/s and network data) has been screened for information that may be relevant to pending or anticipated litigation.

Once litigation is underway or anticipated, counsel will want to move swiftly to locate and place holds on known sources of potentially relevant data. An IT architectural map illustrating the locations of various types of data can be a great help in this process. The alternative, to start from scratch every time a new litigation hits, is costly and inefficient. An effective checklist will address all kinds of data and locations, including both data belonging to individuals and data belonging to groups, such as public folders, team rooms, enterprise applications and discussion databases.

Save Disaster Recovery Tapes for *Disasters*

Part of the initial planning stage should include identifying the kinds of data that are being routinely destroyed and evaluate whether this creates the risk of spoliation in event of litigation.

In deciding what electronic data to preserve, the legal department should carefully consider how data on the company's disaster-recovery backup systems is treated. Modern backup systems can be amazingly complex. Some of the newest systems store hundreds, even thousands, of tapes in silos that are manipulated with robotic arms, with data spread across the tapes for optimal storage. So, an order to "preserve all backup tapes" or retrieve specific data from backups could be extremely expensive, time-consuming, and practically impossible.

Such complex backup systems are not designed for the preservation of evidence or for routine daily use. Their purpose is *disaster recovery*. So even if it is possible to use them to retain and collect data, this fundamentally alters their function from disaster recovery to regular business use or records retention. Nevertheless, it is hard to argue against a sophisticated opponent that your company should not be required to search its "disaster recovery" tapes if it is using them in the ordinary course of its day-to-day operations to retrieve lost documents however "disastrous" the loss may be to an individual user.

Typically, backup tapes are erased and overwritten at pre-set intervals (weekly, monthly). This presumes that the company has a process and policy for preserving designated business records for regulatory purposes. Some companies find themselves in the difficult situation of having backup tapes as their *only* means of preserving electronic data. This creates difficulties because there is no easy way to: 1) dispose of documents when their retention period is up; or 2) access them or preserve them if a litigation hold is imposed.

Implementation and Follow-up

It is a sobering fact that the corporate graveyard is littered with data preservation plans that were never properly followed. Having a plan that is not implemented is worse than having no plan at all. Not only does it give the corporation a false sense of security, but more devastatingly, it gives plaintiff's counsel a documentary roadmap of what the company itself believed it needed to do to comply with legal and regulatory requirements—*but failed to do*—as evidenced by its lack of compliance with its own policy. That is not a battle you want to have to fight.

Thus, simply promulgating the policy is only the start, not the end of the story. There needs to be a structured training program, auditing for compliance on an ongoing basis, updates to accommodate new types of records or changes in retention requirements, and processes for suspending specific document disposition in the event of a litigation hold. In addition, accessibility of data should be an important consideration as the purposes of preserving data for litigation are to: 1) review it for relevance and privilege; 2) produce it to the other side; and of course 3) build your client's case and defenses.

Battle Stations

At the very first sign of litigation, the company should be prepared to act. Such readiness means more than simply having a litigation response plan established in advance. The legal and IT staff must understand the plan and be prepared to take specific steps when the litigation is reasonably likely even if it is not yet a reality.

A good preservation plan needs to include a formal, documented protocol to follow once litigation is underway. Counsel should only need to refer to the procedures for document preservation and gathering that are already in place to develop a plan specific to the particular case. As part of this process, they should undertake the limited acquisition and review of a targeted data sample. Again, this action should be underway as soon as possible and *not* put off until the opponent weighs in on what should be preserved and reviewed. Being ready to present an existing plan puts the company in a much better position.

Furthermore, the plan must be more than just a memo to employees warning them not to delete certain electronic documents. There must be a real plan that includes specific processes on how to actually preserve the data and how to monitor and enforce compliance.

The plan should preserve the potentially relevant data of all those individuals reasonably anticipated to be involved in the litigation, and the preservation notice should go not only to the affected employees but also, as appropriate, to outside vendors who may be the only source of potentially relevant data.

Implementing Litigation Holds

It is important to implement document preservation safeguards as soon as the legal department has reason to suspect that the company will become a party to a legal proceeding. In implementing these safeguards, the company is required to adjust its ordinary retention policies to ensure preservation of records it believes could be the subject of a reasonable search request.

Although the law is not clear on the subject, it was widely believed that a company that inadvertently (rather than intentionally or recklessly) destroyed records related to a pending litigation was not likely to be subject to spoliation sanctions. But a number of court decisions suggest otherwise. For example, in *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2nd Cir. 2002), Judge Cabranes of the Second Circuit Court of Appeals found that negligence alone is sufficient for a finding of spoliation and imposition of sanctions. It is important to note, however, that there is wide disagreement in the courts as to the requirements for a finding of spoliation. A proposed amendment to Rule 37 of the FRCP would create a safe harbor for unintentional destruction of data.

Many companies have no systematic method for the legal department to alert other company personnel (such as the records management and IT departments) that litigation is pending and that special efforts must be made to preserve records. The Cohassett study found that 46 percent of companies have no formal system for "hold orders" to preserve discoverable information and 65 percent do not have a system of hold orders for electronic documents. *2003 Electronic Records Management Survey*, Cohasset Associates.

Defeating a Sweeping Preservation Plan

As an opening shot across the bow, plaintiff's counsel is likely to make sweeping demands for data preservation or even seek an *ex parte* preservation order, claiming that the corporation is planning or is actually in the process of destroying data. The harsh reality is that an unprepared company may be doing just that and not even realize it.

The goal of these demands is often not only to ensure that potentially relevant data is preserved, but also to make the effort to preserve the data so costly that the company considers a less favorable settlement than might otherwise be warranted.

One way to defeat such a preservation demand, or worse—an order—is to demonstrate to the court that the company already has a reasonable and defensible plan underway that will ensure the retention of relevant data. Typically, judges favor sensible plans already in place over vague demands that the corporation preserve everything, relevant or not.

To be fully defensible in court, the plan must show that the company's processes for collecting data will preserve the full content

of the data and will include adequate documentation and quality assurance.

Cut the Volume of Data

In a small case, the number of electronic documents can be in the tens of thousands; in a large, complex case, that number can reach the hundreds of millions or even billions. Even if a company could afford to review so much data manually (which it could not), the process would be so onerous and time-consuming that it would take scores of reviewers years to accomplish.

At this stage of the process, companies will often enlist outside experts to join their data discovery teams. The best of these experts are skilled in defensibly extracting targeted, potentially relevant material from the mass of data, thereby reducing the proverbial mountain to a molehill in a well-documented manner.

Technological advances have made it possible to apply a variety of tools to this process. These tools go far beyond traditional word searches employing techniques such as the searching, classification and selection of data based on semantic analysis; so-called "concept" searching; and the examination of social networks based on communication patterns and linguistic analysis. This process typically requires the experts to work closely with the legal team and other key participants to develop and refine search and selection criteria. A defensible process will entail testing both search "hits" and "non-hits" as well as the ability to refine the criteria as more is learned about the data set and the case. Finally, full documentation of the tools and the processes used is a key to defending any challenge to the process—be wary of the "black box" solution that cannot be explained because it uses "proprietary" technology. That may sound good in a marketing piece but marketing won't get you very far in explaining and defending your choices in court.

What about the Duplicates?

Even if data analysts are able to separate the potentially relevant from the irrelevant, they still face the problem of dealing with duplicate material. A single e-mail that is forwarded to others, copied, backed up and so on, can spawn a long string of duplicates and near duplicates. Reviewing countless duplicates can be both time-consuming and costly.

One common method of de-duplicating involves assigning a unique digital signature using a formula, or *algorithm*, based on the information in the e-mail. This number, or *hash value*, can be compared to other e-mail messages. Any e-mail that has the same value can be safely characterized as a duplicate and removed from the set of data to be reviewed. The Md5 hash value is the most commonly used and was developed by an MIT professor, Ron Rivest, in 1991.

Having a plan that is not implemented is worse than having no plan at all.

But Md5 hashing is not the end of the story when if comes to de-duplication. A further complicating factor is that there are often large volumes of e-mail that are functionally identical for purposes of review—but not precisely the same—thus rendering the Md5 hash values different. For example, there may be multiple copies of the same e-mail with different "sent times." Or, as is often the case, there may be a long thread of e-mail messages that make up a discussion amongst several senders and recipients with additional comments added at each stage. While the messages at each stage of the communication are different, for purposes of review, looking at the last in the string would cover all of the same content as looking at each individual message separately. There is now software capable of identifying so-called "near duplicates" and removing them, if desired, from the review set.

Ongoing Data Preservation

One of the challenges for the legal team is to keep up with the ongoing creation of new documents in the ordinary course of the company's business. Fortunately, software has been developed to automate this process. Such software uses specific selection criteria, such as the identity of the user and the date range of the item, to automatically collect data meeting the criteria and store it in a searchable database. By "collecting and loading" target data proactively, the legal team can eliminate the need to retain all data from everyone involved in the litigation and avoid the costly restoration and searching of disaster backup media.

If They Ask for More

In most jurisdictions, the cost of collecting and providing data is shouldered by the responding party (New York State is one exception). But what if lawyers for the requesting party are unreasonable and demand everything under the sun? The general rule is that a company is required to do only what is reasonable, based on such factors as the amount in controversy in the case, the case schedule and the significance of the issues involved.

If the responding party adopts a reasonable and documented process and implements it, they are in a strong position to argue that anything beyond the reasonable amount undertaken should be borne by the requesting party. Chances are the requesting party will back off.

Wrap-up

Even for a small company, the challenge of preserving electronic data can be formidable. Fortunately, the technology for collecting, searching and preserving electronic data is developing rapidly to meet the demand.

Rather than wait for an unreasonable preservation or production request or risk being sanctioned by the courts for not preserving electronic evidence, companies should take a proactive approach—with the goal of keeping several steps ahead of their opponents. In the long run such an approach can be the most cost-effective. When opposing counsel discovers that your company has the potentially relevant data at its fingertips and can readily defend its process for preservation, collection, review and production of data, they will be far less likely to try to make discovery itself an issue in the case. **FD**