Proactive solutions: the next generation of eDiscovery?

Herbert L. Roitblat, Ph.D.

Discovery has always been an "after-the-fact" process. Much like archeology, pieces of evidence were searched for, reviewed, categorized and logged. By the time Discovery, and more recently eDiscovery, commences, some event or series of events has already (allegedly) happened, and eDiscovery is used as a means to investigate the facts of the situation and produce relevant documents for both parties. Discovery in general, and eDiscovery in particular, is historically post hoc, ad hoc, and expensive. With the exponential proliferation of e-mail and electronic documents, the situation is getting worse, and the burdens of Discovery and eDiscovery are continuing to skyrocket.

As recent cases show, the consequences for failing to meet eDiscovery responsibilities can be substantial. Morgan Stanley was sanctioned for more than $1 billion for having relied on an inadequate, inconsistent, and ineffective methods for archiving and retrieving their data.

Electronic documents also figure prominently in compliance. Corporations may have to demonstrate to their investors that the company is complying with all relevant laws, rules, and regulations. Management may have to show that internal controls are effective at deterring illegal behavior. Among the laws and regulations with which they must comply are antitrust regulations, wire and mail fraud acts, the Federal false-Claims Act, the Foreign Corrupt Practices Act, employment and civil rights regulations, sexual harassment regulations, securities laws, and environmental regulations. Acting proactively to comply with these requirements also provides the means by which eDiscovery can be made more affordable and more effective while also providing a method for finding infractions quickly, enabling the corporation to act to correct situations before they become huge liabilities.

Proactive advantages

In response to the rising tide of data and high risk of litigation, corporate counsel are beginning to seek proactive remedies for their eDiscovery and compliance headaches. The emerging trend will be proactive solutions that offer the ability to be prepared when a matter goes to discovery, rather than have to rush a new solution for each matter. Technology is currently available to manage the information your company accumulates, reduce the volume that needs to be stored, allow counsel to respond quickly and easily to discovery requests, examinations, and investigations, manage holds; and produce documents as needed.

Chief among these proactive solutions is the use of an intelligent email archive to store the company's business emails, along with attachments, and other electronic documents. This archive allows for the analysis of these documents, and thereby, transforms them from a liability into a reusable asset. The general idea is to capture every email that is either sent or received by company employees, automatically categorize those emails according to the company's retention and compliance policies and other controls and then

archive the results as needed. Business records can be stored for the appropriate period. Emails that are judged not to be business records can be scanned for evidence of any noncompliant, fraudulent, or other illegal behavior. Those categorized as non-problematic need not be archived.

Such a system gives the company a view into the activities of its employees and minimizes the number of documents that must be maintained. It provides a consistent set of rules for determining what to keep and what can be destroyed. It allows the company to prepare for litigation, but also provides the opportunity to prevent its necessity in many cases.

Keep clients out of jail

A proactive legal approach emphasizes keeping the company and its employees out of trouble, rather than merely reacting to troubles as they arise. It is usually much easier and more cost effective to take remedial steps to resolve problems early on before they become nightmares, than it is afterward. Federal sentencing guidelines, for example, favor organizations that find evidence of misdeeds within their organization and work to correct them.

Good business practice requires that companies take steps to ensure that their employees comply with company policies as well as with the laws, rules, and regulations that apply to them and their industry. An increasingly important part of that practice involves monitoring and storing electronic documents, including emails and their attachments and managing these documents throughout the information lifecycle. An electronic document may have a direct business use of only a few minutes, perhaps to signal agreement to a contract term. This same document may have an afterlife of many years during which it needs to be retained and managed.

Mitigate risks

Risks need to be identified and mitigated. A proactive compliance program insures that documents that need to be retained are archived and that risks be mitigated effectively. With advancement in technology, corporate counsel can now proactively mitigate the company's risk by scanning for evidence of bad behavior before that behavior becomes a costly legal concern.

The risks of doing business involve not only traditional business decisions, such as whether to build or buy a required widget, but increasingly risks of violating laws and regulations and risks derived from how potential violations are handled. The penalties for certain kinds of violations can be severe. For example, the penalty for knowingly destroying documents relevant to a government investigation can be a $5 million fine and up to 20 years in jail under the Sarbanes Oxley regulations. There is not only a risk that an employee may commit an act for which the company is liable, but there may be a risk derived from how the company reacts to this information.

Under Sarbanes-Oxley, a company must certify that its financial controls are adequate. Under Section 404, management must produce "an assessment, …, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." Given the prevalence of emails in corporate communications and the fact that people are often

sloppy, casual, or irreverent about what they are willing to say in an email, it would seem that analysis of these communications would be an essential part of this assessment.

For example, according to recent studies about half of the corporate frauds that are eventually detected are found by accident or by a tip. Formal financial controls are not adequate in these cases. Your odds can be improved by employing an effective email monitoring system.

Similarly emails are often the focus of sexual harassment claims. Monitoring emails for inappropriate language would make it much easier to uncover cases of potential sexual harassment in the organization and remediate them as quickly as possible.

Rapid response to complaints

Other potential sources of expense in eDiscovery include the effort required to collect the electronic documents for processing and the delay while these data are processed. Electronic data are stored in many locations, including individuals' desktop computers, distant office locations, and even employee's home computers. The cost and effort required to gather all of these documents can be substantial. In addition, gathering these documents takes time, during which expenses may mount, the impact of required holds may force extra expenses (for example, because backup tapes may not be reusable during a hold), and the chances for an expedient settlement are delayed. You have to wait until documents are collected even to know what your exposure is. An effective archive can reduce the time and expense required to gather data and make an assessment.

Budgetable, reusable

Having an electronic document repository makes eDiscovery a budgetable, manageable process. By managing corporate communications and electronic documents proactively, corporate counsel can reduce the volume of information that is potentially subject to discovery, reduce the cost of collecting and providing this information to outside counsel or opposition parties, and allow their outside counsel to spend a greater percentage of their time on legal issues rather than on the collection and ad hoc management of eDocuments.

Data contained in a repository do not need to be collected or processed again in order to be reused in a new matter. The data are immediately accessible so you do not have to endure long delays just to find out what your exposure is.

Your outside counsel will not have to spend time designing an eDiscovery collection plan or seeking bids for processing electronic communications and documents. They can focus on managing the legal strategy of the case rather than the "plumbing" of handling and processing documents.

Holds

Complying with hold orders will no longer bring your company's IT program to a halt. Because your electronic documents are in a repository, all it takes to implement a hold is to halt the deletion of these records from the repository. Your ongoing email and disaster recovery systems can continue unchanged. Ongoing business processes will not be affected. Prospective holds, in which you need to collect and avoid destruction of future

emails and other documents can also be implemented specifically within the repository because documents are being collected on an ongoing basis. The repository gives greater reliability that the appropriate documents are being maintained and at the same time, ensures negligible impact on your day to day processes.

Manage volume, Minimize what is stored

One reason that eDiscovery is so expensive is the high volume of irrelevant, personal, and otherwise non-responsive emails and other electronic documents that accumulate in the average company. More than 90% of the average company's communications are electronic. These include both the business related ones, and personal emails, comments, and other documents that go far beyond the scope of business documents that were retained before electronic documents took over the business world. When dealing with paper based documents, the limited space available for filing cabinets was a strong incentive to save only the documents that were actually needed. Employees had to make an effort to file a document. With electronic documents, the opposite is true. There is very little incentive to discard an email message, early draft, or other electronic document. They do not take up perceptibly more space in the office. Rather than having to decide to keep a document, employees have to make an effort to delete electronic documents.

A proactive system has to provide tools to manage what electronic documents are saved and for how long. Not every electronic document has to be saved, though some organizations have descended the slippery slope of trying to keep them all. Saving all emails is not a scalable strategy. Saving everything does not mean that you can find it again. It is incredibly difficult to guess the right terms to search for that find the documents you need and do not swamp you with irrelevant ones. Making the effort to keep your repository orderly and relevant will pay huge dividends when the information is needed.

Using rules and other queries is a very useful part of keeping your repository in order. If any questions arise as to how the documents were selected, the rules can be produced as evidence that the decisions were made systematically and reliably. Employees are likely to be inconsistent in how they categorize documents for retention. Studies have found that people agree on how to categorize documents less than 50% of the time. More importantly, employees are often slipshod in their categorization because they have to stop their "day" jobs in order to do their compliance/retention jobs. They often see compliance as a burden that interferes with their regular work.

Minimize spoliation claims

With data in a repository, you don't have to repeatedly pay to process the same data or worry that your eDocuments will be destroyed with the next backup tape recycling. There are no more worries that these documents will be misplaced in a closet somewhere, only to appear by accident partway through the discovery process.

There has been a lot of attention devoted to the consequences of spotty procedures and systems for retaining email. Companies have been fined millions of dollars for not being able to produce emails, which their policy would have mandated saving, in a timely

manner. Others have been fined for deleting emails after they were notified that these documents might be relevant in a pending lawsuit.

Conclusion

An emerging trend in electronic discovery will be proactive solutions that offer the ability to be prepared when a matter goes to discovery, but also help avoid going to the courts to at all. Corporate counsel faces the challenge of dealing with the ever-increasing burden of electronic discovery. Having a repository of business documents and monitoring all electronic communications will be instrumental in meeting that challenge in a cost-effective way. Repositories may appear to be expensive to set up, but consequences of not using one can be even more crushing.

Data that are inconsistently retained can lead to the production of accusatory documents without the potentially exculpatory context that other documents may provide. It makes it easier for the other side to request documents, but it also makes it easer for the company to assess their exposure and because the documents are being monitored for risky, inappropriate, illegal, or noncompliant behavior, the repository may substantially decrease the frequency with which the company appears in court. The value of that may be priceless.

Unfortunately, many corporations can expect a steady stream of lawsuits year after year. Many of these lawsuits repetitively require some of the same discovery which may or may not yield the same documents in each matter, thus introducing yet another potential liability. In the case of public companies a typical example could be numerous class action lawsuits, which can be filed in multiple jurisdictions, with multiple classes, all having to be handled separately until they are either consolidated or settled. A proactive repository could save millions of dollars in costs and even more in further liability avoided.

Lawyers of the 21st century need a much broader and proactive perspective when it comes to data and electronic evidence than they have had. The lawyer of the future will need to be prepared in order to offer the best possible service to their clients, or risk losing them to someone who can.

About the Author:
Herbert L. Roitblat, Ph.D. is DolphinSearch's Chief Scientist, co founder, and primary inventor and patent holder of the core DolphinSearch Neural Network technology. Dr. Roitblat was an award-winning Professor of Psychology at the University of Hawaii from 1985 until 2002. He received his BA Degree from Reed College in Portland, OR and his Ph.D. in Psychology from The University of California-Berkeley. In addition to his scientific work, Dr. Roitblat has been writing extensively about the problems of dealing with massive amounts of electronic data and the emerging standards for dealing with those problems. He is a member of the Sedona working group on Electronic Document Retention and Production.
www.dolphinsearch.com