ESSENTIAL CALIFORNIA LEGAL CONTENT | WEEK OF DECEMBER 24, 2012 | VOL. 136, NO. 52 An ALM Publication

THE RECORDER

IN PRACTICE

Defensible Deletion

Companies will have to innovate and develop plans for dealing with massive amounts of electronically stored information

Philip Favro

When Kolon Industries Inc. found itself on the wrong side of a $919 million verdict last year, the South Korean-based manufacturer probably started to take inventory on what it might have done differently to have avoided such a fate. While that list could have included any number of entries, somewhere near the top had to be an action item to revamp its information retention policies and litigation hold procedures. Breakdowns in those protocols led to the destruction of nearly 18,000 pages of electronically stored information, or ESI. This, in turn, resulted in a corresponding instruction to the jury in *E.I. du Pont de Nemours v. Kolon Industries*, 803 F.Supp.2d 469, that Kolon had engaged in wholesale destruction of key evidence. This eventually culminated in a devastating verdict against the manufacturer.

Most companies fortunately will never have to deal with the fallout from a nearly $1 billion verdict. Nevertheless, they still struggle with the same cost and logistics issues associated with information retention that ultimately tripped up Kolon Industries. While there are no quick or easy solutions to these problems, an ever increasing method for effectively dealing with them is through an organizational strategy referred to as defensible deletion. A defensible deletion strategy could allude to many items.

> **'Defensible deletion is a comprehensive approach companies implement to reduce the storage costs and legal risks associated with the retention of ESI. '**

But at its core, defensible deletion is a comprehensive approach companies implement to reduce the storage costs and legal risks associated with the retention of ESI. Organizations that have done so have been successful in avoiding court punishment while at the same time eliminating ESI that has little or no business value.

DEVELOPING AN OVERALL STRATEGY

Most companies tend to agree that adopting a defensible deletion strategy makes business sense. Indeed, in a recent industry survey, 70 percent of respondents agreed that such a strategy is critical to reducing the costs and risks associated with information retention. Despite the perceived benefits of defensible deletion, other surveys confirm companies are still delaying implementation of the procedures that would enable this strategy. This is often the result of many factors. For example, organizations often do not have information retention policies. In many enterprises, the key stakeholders responsible for defensible deletion — lawyers and IT professionals — frequently have trouble working together. Yet without these elements, companies unwittingly delegate to their rank-and-file employees the duty to manage, archive and discard data. Allowing employees to arbitrarily manage company information is often disastrous.

Thus, the first step to implementing a defensible deletion strategy is for organizations to ensure that they have a top-down plan for addressing data retention. This typically requires that legal and IT are cooperating with each other. These departments must also work jointly with records managers and business units to decide what data must be kept and for what length of time. All such stakeholders in information retention must be engaged and collaborate if the organization is to create a workable strategy.

This is especially important for email. Email (and its destruction) generates more e-discovery headaches than any other source of information. But the answer to this problem is not to keep all company email. That would cause an organization to needlessly increase operating expenses while stockpiling useless and in some cases risky information. Instead, legal and IT should set a period for retaining email that is reasonable in relation to the enterprise's business, industry and litigation profile.

Cooperation between legal and IT naturally leads the organization to establish records retention policies, which carry out the key players' decisions on data preservation. Such policies should address the particular needs of an organization while balancing them against litigation requirements. This will enable a company to reduce its costs by decreasing data proliferation. In addition, it will minimize a company's litigation risks by allowing it to limit the amount of potentially relevant information available for future litigation.

USING TECHNOLOGY TO FACILITATE DEFENSIBLE DELETION

In the digital age, an essential aspect of defensible deletion is technology. Without it, organizations cannot realistically expect to reduce data volume and the resulting legal exposure of that data.

> **'An essential aspect of defensible deletion is technology. Without it, organizations cannot realistically expect to reduce data volume and the resulting legal exposure of that data.'**

A particularly useful innovation that can help address the costs and risks of stockpiling data is archiving software. A software archive provides organizations with a central repository to manage company ESI. One of the critical functions of that repository is data classification. Classification tools analyze and tag data content as it is ingested into the archive. Depending on the content, categorized ESI may be assigned a particular retention period or may be flagged for deletion. By so doing, organizations may retain information that is significant or that otherwise must be kept for business, legal or regulatory purposes — and nothing else. They can also search for data with greater efficiency, which will help reduce expenses downstream when documents must be retrieved in response to legal demands.

A central archive can also reduce costs through efficient data storage. For example, the repository's automated processes can expire data in accordance with retention policies. In addition, many archives employ deduplication technology, which preserves only a master copy of each document. By storing only one copy of a document, archives free up space on company servers for the retention of other materials and ultimately lead to decreased storage costs.

Archiving software can further diminish legal risks by helping remove information management decisions from the exclusive control of rank-and-file employees. While employees can use the software to access their archived email and other ESI, it can be programmed to prevent employees from deleting or modifying that data. This is significant since employees may be tempted to conceal their errors. Moreover, ordinary employees may lack the depth of corporate knowledge necessary to determine what documents must be retained for business, legal or regulatory purposes.

And by relying on an automated process rather than employees to manage and expire data, an organization may further reduce litigation risks through the "safe harbor" for the destruction of electronic information under Code of Civil Procedure §2031.320(d) and Federal Rule of Civil Procedure 37(e). Those provisions are designed to protect organizations from court sanctions when the ordinary, good faith operation of their automated systems causes email, archival data and other electronic information to be overwritten and destroyed. The automated processes of a software archive, which expire ESI pursuant to company retention policies, dovetail with the safe harbor's requirements.

DEVELOPING AN EFFECTIVE LEGAL HOLD PROCESS

Another critical aspect of a defensible deletion strategy is the development of an effective legal hold process for e-discovery purposes. Like the creation of ESI retention policies, the legal department should work cooperatively with IT to create a protocol for how the organization will address document preservation in response to legal and regulatory actions. Such a process will likely involve the designation of officials who are responsible for issuing a timely and comprehensive litigation hold. This will better ensure that ESI subject to a preservation duty is actually retained and thereby help an organization avoid the mistakes that often characterize e-discovery both before and during litigation.

USING AN E-DISCOVERY PLATFORM TO ENABLE LEGAL HOLDS

To facilitate the legal hold process, organizations should consider deploying an e-discovery platform with the latest in legal hold technology. E-discovery platforms can enable automated legal hold acknowledgements on various custodians across multiple cases. Such functionality allows organizations to confidently place data on hold through a single user action. This, in turn, eliminates concerns that ESI may slip through the proverbial cracks of manual hold practices.

To enable a strategic and seamless legal hold placement on ESI, the e-discovery platform should also be compatible with the software archive. Such integration allows an organization to efficiently suspend aspects of its automated retention policies. In addition, it enables parties to quickly identify and collect pertinent ESI from the archive for immediate processing, search and analysis without the costly and time-consuming involvement of third party vendors.

Finally, a platform should also provide transparency regarding user actions. Such transparency ideally would enable an organization to establish a chain of custody for each email, document or file across the entire spectrum of information governance. All of which has the effect of obviating costly investigations that are often required to address an organization's information retention practices and e-discovery review efforts.

CONCLUSION

Organizations are experiencing every day the costly mistakes of delaying implementation of a defensible deletion program. While they may not necessarily result in a $919 million verdict, those mistakes are wasting precious company resources at the expense of innovation and revenue. Fortunately, this trend can be reversed through a commonsense strategy which, when powered by effective, enabling technologies, can help organizations decrease the costs and risks associated with the information explosion

In Practice articles inform readers on developments in substantive law, practice issues or law firm management. Contact Vitaly Gashpar with submissions or questions at vgashpar@alm.com.

Philip Favro brings over thirteen years of discovery expertise to his position as Discovery Counsel for Symantec Corp. Phil is a speaker, author, blogger and consultant on the challenges that electronic data have imposed on information retention and eDiscovery practices, and how to address those challenges in legal matters. Phil's expertise has been enhanced by his practice experience as a commercial litigation attorney in which he advised a variety of clients regarding complex discovery issues.