The Golden Rules of E-Discovery

Gaining the Advantage in Litigation

By Philip Favro, Discovery Attorney, Symantec Corporation

The e-discovery frenzy that has gripped the American legal system over the past decade has become increasingly expensive. Particularly costly to organizations is the process of preserving and collecting documents. These aspects of discovery are often lengthy and can be disruptive to business operations. Just as troubling, they increase the duration and expense of litigation.

Because these costs and delays affect clients as well as the courts, it comes as no surprise that judges have now heightened their expectation for how organizations store, manage and discover their electronically stored information. Gone are the days when enterprises could plead ignorance for not preserving or producing their data in an efficient, cost-effective *and* defensible manner. Organizations must now follow best practices—both during and before litigation—if they are to navigate the stormy seas of e-discovery.

Fortunately, the courts have not left litigants to grope blindly for direction. Particularly in 2011, the judiciary has provided a roadmap for what type of best practices organizations should implement to effectively address e-discovery. And while there were many lessons the courts imparted, three stand out in particular as the "golden rules": (a.) Issue a timely and comprehensive litigation hold; (b.) suspend aspects of document retention policies; and (c.) manage all stages of the document collection process.

The Three Golden Rules

1. ***Timely litigation hold.*** The first of these rules is also the most important: issue a timely litigation hold. The need for a litigation-hold process arises when litigation is pending or is reasonably foreseeable under the circumstances of a given case. The hold is the first step required to ensure and enable the preservation of pertinent evidence for litigation.

Without a timely hold instruction, the entire discovery process may very well collapse. For documents to be produced in litigation, they must first be preserved. And they cannot be preserved if the key players or data source custodians are unaware that they must be retained. Indeed, employees and data sources may discard and overwrite electronically stored information if they are oblivious to a preservation duty. The failure to issue a proper hold instruction thus leaves organizations vulnerable to data loss and court punishment. No case is more instructive on this issue from 2011 than E.I. du Pont de Nemours v. Kolon Industries (E.D. Va. July 21, 2011).

"Organizations must now follow best practices if they are to navigate the stormy seas of e-discovery."

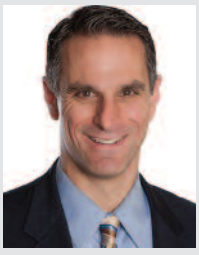
In *DuPont*, the court issued a stiff rebuke against defendant Kolon Industries for failing to issue a timely and proper litigation hold. That rebuke came in the form of an instruction to the jury that Kolon executives and employees deleted key evidence after the company's preservation duty was triggered. The jury responded by returning a stunning $919 million verdict in favor of DuPont.

The destruction at issue occurred when Kolon deleted emails and other records relevant to DuPont's trade secret claims. After being apprised of the lawsuit and then receiving multiple litigation hold notices, several Kolon executives and employees met together and identified emails and other documents that should be deleted. The ensuing data destruction was staggering. Nearly 18,000 files and emails were deleted. Furthermore, many of these materials went right to the heart of DuPont's claim that key aspects of its Kevlar formula were allegedly misappropriated to improve Kolon's competing product line.

Surprisingly, however, the court did not blame Kolon's employees as the principal culprits for spoliation. Instead, the court criticized the company's attorneys and executives, reasoning they could have prevented the destruction of information through an effective litigation-hold process. The three hold notices circulated to the key players and data sources were either too limited in their distribution, ineffective since they were prepared in English for Korean-speaking employees, or too late to prevent or otherwise alleviate the spoliation.

The *DuPont* case underscores the importance of the timely issuing of an effective litigation hold. As *DuPont* teaches, organizations should identify what key players and data sources may have information. A comprehensive notice should then be prepared to communicate the precise hold instructions in an intelligible fashion. Finally, the hold should be circulated immediately to prevent data loss.

Organizations should also consider deploying the latest technologies to help effectuate this process. This includes an e-discovery platform that enables automated legal hold acknowledgements. Such technology will allow custodians to be promptly and properly notified of litigation and



Philip Favro

Philip Favro is a discovery attorney for Symantec Corporation in Mountain View, CA. Favro brings to Symantec practical expertise in electronic discovery. He has advised technology companies and other clients regarding complex e-discovery issues during his 11-year litigation practice. Favro's research addresses the changes and challenges that electronic data have forcibly introduced into litigation and, in particular, on discovery practice. He now works with Symantec customers and company stakeholders on information governance and e-discovery matters. Favro is also a member of the Electronic Document Retention and Production (WG1) Working Group of the Sedona Conference.

thereby retain information that might otherwise have been discarded.

Coupling an e-discovery platform with an effective archiving solution can also strengthen the legal-hold process. Archiving software can be programmed to prevent employees from deleting emails and other electronically stored information. By ingesting data into a central repository and leaving copies of the materials on local computers, employees can have access to their archived records. They cannot, however, delete those documents from the software archive. In addition, a litigation hold can be placed on archived data to prevent automated retention rules from overwriting information. Either of these features might have prevented much of the spoliation—and resulting sanctions—that occurred in the *DuPont* case.

2. *Suspending document retention policies.* The next golden rule of e-discovery involves suspending aspects of document retention policies to ensure preservation of relevant information. This goes beyond placing a hold on archival data. It requires an organization to identify the data sources that may contain relevant information and then modify aspects of its retention policies to ensure that data is retained for e-discovery. Taking this step will enable an organization to create a defensible document retention strategy and be protected from court sanctions under the Federal Rule of Civil Procedure 37(e) "safe harbor" provision.

Rule 37(e) shields litigants from sanctions even though their data has been destroyed pursuant to the routine operation of their electronic information systems. Described in layman terms, organizations may avoid court punishment even though their computer systems deleted email and other electronic data. To find shelter in the safe harbor, however, courts require that the "routine operation" be carried out in "good faith." This typically entails modifying or suspending aspects of a retention policy when a preservation duty attaches. The decision from Viramontes v. U.S. Bancorp (N.D. Ill. Jan. 27, 2011) is paradigmatic on how organizations can avoid sanctions under Rule 37(e) by suspending aspects of retention policies.

In *Viramontes*, the defendant bank defeated a sanctions motion because it modified aspects of its email retention policy once it was aware litigation was reasonably foreseeable. The bank implemented a retention policy that kept emails for 90 days, after which the emails were overwritten and destroyed. The bank also promulgated a course of action whereby the retention policy would be promptly suspended on the occurrence of litigation or other triggering event. This way, the bank could establish the reasonableness of its policy in litigation. Because the bank followed that procedure in good faith, it was protected from sanctions under Rule 37(e).

As the *Viramontes* case shows, an organization can be prepared for e-discovery disputes by timely suspending aspects of its document retention policies. By creating and then faithfully observing a policy that requires retention policies be suspended on the occurrence of litigation or other triggering event, an organization can develop a defensible retention procedure.

3. *Effectively managing the document collection process.* A third best practice the courts emphasized in 2011 is the importance of effectively managing the document collection process. That means uncomfortable corporate bedfellows—the legal and IT departments—will need to cooperate if they are to ensure that data collections are properly carried out. Without the cooperative supervision from both legal and IT, organizations unwittingly delegate to their rank and file employees the duty to identify, preserve and collect relevant information. Allowing employees to unilaterally and arbitrarily do so is generally a recipe for disaster. Such a *laissez-faire* practice typically prevents an organization from preserving and collecting relevant data from custodians and data sources. Moreover, it undermines the credibility and effectiveness of the e-discovery process.

> **"Coupling an e-discovery platform with an effective archiving solution can also strengthen the legal-hold process."**

Not surprisingly, courts frequently fault organizations that delegate the responsibility for the collection process to their employees. The case of Green v. Blitz U.S.A., Inc. (E.D. Tex. Mar. 1, 2011), is a quintessential example of the problem of letting employees have the "last word" on these issues.

In *Green*, the defendant company was sanctioned for failing to properly identify, preserve and collect relevant electronic information. The company lost key emails after entrusting a single, lay employee with the identification and collection of discoverable documents. That employee had little if any supervision from legal counsel. Worse, the employee failed to involve IT in the production process despite his lack of technical sophistication. As a result, entire categories of relevant data were destroyed and the company was sanctioned accordingly.

Similarly, in Northington v. H & M International (N.D.Ill. Jan. 12, 2011), the court issued an adverse inference jury instruction against a company that destroyed relevant emails and other data. The spoliation occurred in large part because legal and IT were not involved in the production process. For example, counsel was not actively engaged in the critical steps of preservation, identification or collection of electronically stored information. Nor was IT brought into the picture until 15 months after the preservation duty was triggered. By that time, rank and file employees—some of whom were accused by the plaintiff of harassment—had stepped into this vacuum and conducted the process of identification, preservation and collection without meaningful oversight. Predictably, key documents were never found and the court had little choice but to promise to inform the jury that the company destroyed evidence.

An organization does not have to suffer the same fate as the companies in the *Green* and *Northington* cases. It can take charge of its data during litigation through cooperative governance between legal and IT. After issuing a timely and effective litigation hold, legal should typically involve IT in the collection process. Legal should rely on IT to help identify all data sources—servers, systems and custodians—that likely contain relevant information. IT will also be instrumental in preserving and collecting that data for subsequent review and analysis by legal. By working together in a top-down fashion, organizations can better ensure that their e-discovery process is defensible and not fatally flawed.

Following these three golden rules will help an organization build a defensible e-discovery process. Adherence to these practices will likewise minimize risks and decrease costs. All of which will ring true with the expectation of courts and clients alike that discovery be conducted in an efficient, cost-effective and defensible manner. ■

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.