

## The Calm Before The Litigation Storm

### *Addressing the Risk Of e-Discovery*

By Adam I. Cohen

Lawyers representing enterprises with complex information systems generating and storing vast amounts of data are familiar with the perils of e-Discovery. If this familiarity did not arise before Dec. 1, 2006, it certainly arrived with the e-discovery clarifications and codifications to the Federal Rules of Civil Procedure (“FRCP”) that took effect on Dec. 1, 2006. Given the implications of these rules for compliance, it is imperative that businesses accelerate and elevate their planning for how to address every phase of electronic discovery — identification and preservation, collection, processing, analysis and production. Unfortunately, dealing with these issues is not as simple as shopping for software packages or asking a

consultant to apply industry best practices to the company’s electronically stored information (“ESI”) procedures. This article spells out a rational, comprehensive plan for achieving e-discovery preparation.

There is no magic bullet for bringing about e-discovery readiness, although there are many peddlers of “solutions” to the new FRCP that would have you believe otherwise. Readiness requires a combination of legal, technical, and practical measures that can only be determined through the application of judgment, preferably informed by experience, to the particular needs of each organization. The idea that there is a universally applicable ESI solution, whether technical or procedural, is pure snake oil.

### **METHODOLOGY**

However, the methodology for achieving e-discovery readiness is not mysterious. It requires experience and action on both proactive and reactive fronts. Neither by itself is sufficient, but both are necessary. Proactive attention to the problem involves conducting fact-gathering investigations, analyses and recommendations encompassed in the readiness methodology. Reactive experience involves understanding the impact of corporate systems,

policies, procedures, and practices on an e-discovery process under a variety of scenarios, including different types of litigation, regulatory queries or internal investigations.

### **Fact Gathering**

For example, consider fact gathering. The starting point for e-discovery readiness is gathering the information necessary to identify and describe each source of ESI that is under the custody or control of the organization. This should include anything that may impact the ability to preserve, acquire, search, process or produce information from those sources.

Typically, such information gathering involves interviews with knowledgeable IT personnel responsible for those various sources of information as well as gathering whatever documentation exists for those systems or repositories. It should be noted that conducting these interviews properly, not to mention incorporating the resulting information into a plan for dealing with the technology at issue, requires technical expertise. However, technical expertise alone is not enough. Because this technical expertise must be applied to the litigation environment expertise in the legal discovery process is also essential. Interviews of company

---

**Adam Cohen** is a senior managing director in FTI Consulting’s Technology practice and is based in New York. Prior to joining FTI, Cohen was a litigation partner at Weil, Gotshal & Manges LLP. He is co-author of a treatise which has been cited as authority in several landmark electronic discovery opinions by federal courts. The views expressed in the article are held by the author and are not necessarily representative of FTI Consulting, Inc.

managers and other users of ESI also may be necessary, depending on the nature of the organization, its information policies and its controls. Ultimately, user practices and needs should be driving the company's overarching IT architecture and operation, not concern about e-discovery. While the whole point of an e-discovery readiness assessment is to determine what adjustments may be needed from the legal department's perspective, these adjustments must take into account the habits of the company's users and whether any proposed changes can reasonably be expected to take root and be effective.

The knowledge acquisition phase does not end with understanding the IT environment relating to electronic preservation and discovery. It is also necessary to get answers about the organization's typical litigation risk profile and regulatory environment because these will provide a look into expected e-discovery scenarios. For example, e-discovery readiness must take into account whether there are company databases relevant to common legal problems, such as a human-resources database system operated by a company with significant employment litigation cases.

### ***Examine the Sources***

Once the universe of company information sources is identified, it is necessary to examine each ESI source to determine how to physically implement litigation hold procedures. While there is a level of procedural documentation that should be higher, it is imperative to outline the general process of information flow and decision-making regarding the "trigger," scope of the preservation duty and implementa-

tion of a litigation hold. Once that is achieved, it is necessary to focus in a more granular fashion on how each source of ESI will be handled. This will avoid unpleasant surprises when a live situation occurs.

### ***Data Collection***

After the triage of high-priority tasks that lay out a map of ESI sources and allow an organization to determine the best method of achieving preservation for each source, an organization can move on to other aspects of the e-discovery process. For example, consider the issue of data collection in litigation. While there is a growing awareness that the method of collection can impact the evidentiary integrity of the target electronic information, many clients still prefer to handle such collection internally, citing cost reasons in some cases. The organization may need policies defining the criteria that will be used in evaluating when to use internal resources for collection as opposed to hiring computer forensic experts. More generally, the organization may want to issue policies regarding the hiring of technology vendors (*e.g.*, outside counsel may not be allowed to do so without first obtaining permission from designated in-house legal department personnel). Apart from policies, there may be technology available for implementation that helps search or manage information for e-discovery and possibly other purposes.

Most companies already have overarching document retention policies, but they also tend to be out of date, unknown to the custodians and not monitored for compliance. e-Discovery readiness requires a review of these policies

to ensure that they are comprehensive and understandable as well as practical from an implementation standpoint. User-custodians need to be trained so that they understand and will implement the policies correctly.

### ***Monitoring and Enforcement***

Finally, monitoring and enforcement mechanisms must be determined. All of the tasks in connection with corporate document retention policies will enable a company's documents to become assets as opposed to liabilities. As a rich history of case law showed even before the advent of the new FRCP, a policy that is not implemented at all or only randomly enforced raises questions about missing documents that can be hard to credibly answer.

### **CONCLUSION**

The overall path to e-discovery readiness may sound simple, but the devil is in the details. Don't make the mistake of paying for a "solution" to the new FRCP that works "automagically." While getting to the point of readiness may require some focused time and expertise, the peace of mind resulting from risk mitigation via a thorough, well-reasoned approach is worth the effort and expense.

