New Jersey Law Journal

VOL. CXCII - NO.11 - INDEX 874 JUNE 16, 2008 ESTABLISHED 1878

Complex Litigation & E-Discovery

# Satisfy Your Company's E-Discovery Obligations

## Create a safe harbor for electronically stored information by taking proactive measures

**By Fernando M. Pinguelo and Rob Kleeger**

A recent survey of 200 United States commercial businesses conducted by Canvasse Opinion found that almost half of the companies do not have a strategy or policy in place on how to deal with electronically stored information (ESI) in litigation or in internal investigations. Even after a year-and-a-half of sensational headlines, e-discovery appears to remain an afterthought in many corporate minds.

However, there is little doubt that electronic communication continues to present significant challenges to companies and their leaders. The challenges relate to the proper handling of electronic communications and the consequences of sloppy document management. These challenges make it necessary to establish the best practices for e-mail retention and production. We all recognize how important these challenges are, but many are paralyzed from doing anything about them because they perceive the development of a proper response to be a daunting task.

What makes ESI so challenging is its volatility. By its very nature, ESI easily can be modified, overwritten, or deleted by normal, everyday use. Routine acts like recycling backup tapes, opening and closing a file, rebooting a computer, modifying a document, or running a daily maintenance program can alter or permanently destroy data. Take those intrinsic qualities, and add the "human factor" and common realities such as the increased volume of data, disorganized or nonexistent record retention practices, numerous storage locations of ESI, and routine purging, and you have what amounts to a formula for a disaster waiting to happen.

While reported cases about e-discovery abuses usually involve extremes, they do offer insight into what can go terribly wrong with poor electronic communication protocol. In *Qualcomm v. Broadcom*, F.Supp.2d, 2007 WL 935617 (S.D.Cal.), for example, a California federal court took Qualcomm and its counsel to task for failing to turn over damaging e-mail evidence. Initially, the court ordered Qualcomm to pay Broadcom's $8.5 million legal fees and referred Qualcomm's attorneys to the local ethics board for an investigation into their conduct.

Because paper files and multiple versions of hard copy are becoming a thing of the past, federal and state courts have amended procedural rules to recognize this trend, and have included new obligations on lawyers and businesses (no matter how big or small) regarding ESI. The new e-discovery rules represent the federal and state courts' attempt to address real-life problems faced by trial lawyers in dealing with rapidly spawning electronic records.

The impact of these new court rules goes far beyond those lawyers and businesses actively involved in a particular lawsuit; yet businesses continue to remain unprepared to meet their ESI obligations. The importance of e-mail in today's corporate world is undeniable. Approximately 541 million workers worldwide rely on e-mail communications to conduct business. It is estimated that corporate users send and receive an average of 133 messages per day. Nevertheless, the Canvasse survey also found that only 25 percent of

*Pinguelo is a litigation partner with Norris McLaughlin & Marcus in Bridgewater and Co-Chair of the firm's Response to Electronic Discovery and Information (REDI) Group. Notably, Pinguelo was involved in New Jersey's first case addressing its new e-discovery rule amendments, and has lectured at the Judicial College of New Jersey on the topic. Kleeger is a Managing Director at The Intelligence Group, a business investigation and intelligence services firm in Bedminster. Kleeger routinely develops early-stage complex digital investigation services for law firms, corporations, HR professional, and other litigation support professionals.*

respondents claim to be very knowledgeable of case law and developments relating to ESI.

These staggering statistics expose CEOs and other business leaders to risk when their organizations lack policies on handling ESI even though they may not be involved in the company's day-to-day IT operations and document management. Having dealt with dozens of C-level executives, general counsel, and IT and HR managers, we have identified three of the most common perceived obstacles that prevent a company from approaching its ESI obligations in a proactive, effective way: (1) lack of interest in the subject, (2) lack of time, and (3) not knowing where to begin to tackle what is perceived to be a daunting task. (We used to think lack of resources was an obstacle, but it is not, simply because the costs associated with preparation are relatively minimal). Senior-level executives must move beyond these obstacles, real or perceived, and take control of the issue and position the company to be ready for what lies ahead.

Here are three important steps you can take today to: "Be Prepared."

### First Step: Form Your Own E-discovery Taskforce

A C-level executive in each company should create his or her own e-discovery taskforce within the organization and charge the taskforce with the responsibility of learning where its ESI is stored, who is responsible for its maintenance, and how it may be accessed; and developing a plan that details what the company will do when it is asked to produce ESI related to a lawsuit or investigation. At a minimum, the e-discovery taskforce should be comprised of at least one in-house attorney, an IT manager and a risk or compliance officer. Ideally, an HR manager and C-level executive should also be members of the e-discovery taskforce. While ultimately the C-level executive will be held responsible for any ESI mishaps, the taskforce will help ensure that the company is protected.

### Second Step: Commission a Written Policy

The e-discovery rule amendments require businesses to: (1) understand their technology and keep track of ESI; (2) suspend any routine ESI deletion policies when a lawsuit is anticipated or risk exposure to severe sanctions; and, (3) be aware of the new obligations imposed upon them. Having a written ESI policy specifically tailored to your ESI situation is critical. Your e-discovery Taskforce should be charged with creating your company's written ESI policy.

Due to an ever growing body of guidelines and rules at both the state and federal levels, corporations must now identify, hold, manage, and produce potentially relevant information and records more rapidly than ever. A good policy is one that reduces an organization's exposure to risk and puts it in compliance with regulations. Organizations that do not develop, communicate and enforce formal policies guiding e-mail behavior and ESI storage are putting their employees and organization at serious financial risk, accusations of fraud, lawsuit filings, damage to reputation, loss of business and decreased productivity.

To effectively manage the risks of ESI, a business needs to develop a set of formal policies that guide the use of ESI, such as e-mail, electronic documents, CRM databases, proprietary databases, instant messaging, PDAs, cell phones, voiceover IP, etc. An effective policy is one that provides specific rules for acceptable use of a company's digital assets, and one that addresses the use of business and personal e-mail, the retention and destruction of data, the forwarding of confidential documents, and acceptable language and content of ESI, among other things.

A policy should also identify required retention periods and any e-mail monitoring processes. Usually, outside experts are effective in assisting a company in addressing these issues because they work closely with managers and can help tailor a policy that recognizes the realities of a business while at the same time protect the company by mitigating the company's risk. For example, many companies do not have a policy addressing the use of a data "wiping program." Wouldn't you want to know if ESI had been destroyed by a former employee prior to paying a severance or negotiating a settlement? The best policies are those that enable a company to access information in an efficient way.

### Third Step: Implement the Policy and Tell Everyone About It Routinely

Having a written policy and then sticking it in a desk drawer will not satisfy your company's obligations. Charge your e-discovery taskforce with the task of notifying employees of the policy through some formal means, such as an interoffice memorandum from a high-level executive that summarizes the policy, explains its importance and details the responsibilities and expectations to which each employee will be required to adhere. Some form of training that will educate employees on their responsibilities should follow the issuance of the memorandum. Courts are acutely aware that a policy is only as effective as its implementation. Policies must be implemented and followed consistently. If there are any deviations, be certain they are justified before they are permitted.

One of the most significant challenges facing companies in the next five years is the proliferation of unmanageable volumes of ESI. That concern, coupled with the fact that the law on e-discovery remains largely unexplored, especially in state courts, should motivate corporate action related to these issues. Moreover, the rules do provide protection against sanctions for a party's inability to provide ESI that has been lost due to routine operations of an ESI system. However, this safe harbor is only available to those who have taken proactive measures, such as the ones detailed above, to address many of the issues surrounding ESI.

The rules place a significant premium on knowledge and preparation. Principles of basic fairness, good records management, an understanding of your data and devices, and professional guidance will likely be the hallmarks in these changing times. ■