Avoiding a Minefield: Managing Electronic Records in a Litigious World

Lowell H. Patterson, III

For those of us who started their working careers with a desk calendar and a Rolodex, the computer age brought almost unimaginable information management capabilities and convenience. For those in the construction industry, these innovations have proven especially useful. Almost every facet of construction has been positively affected by the advancement in information related technology. Many formerly time-intensive and expensive tasks may now be accomplished in a fraction of the time formerly required with relatively little expense. Interconnecting Blackberries, desktop computers and remote access laptop computers have unleashed significant benefits, including information utilization efficiencies and enhanced and inexpensive internal and external communication. As with every technical advance there is some related pitfall or risk.

A by-product of increased computer usage involves the creation of enormous amounts of electronic data which must be maintained, managed and properly discarded. A project may generate numerous internal and external email communications by, between or among a wide variety of persons including owners, contractors, sub-contractors, vendors and other third parties. When disputes, investigations or litigation arise, some of these communications may be highly relevant. The willful or even the inadvertent destruction of electronic data or records can result in serious and potentially very costly consequences. Through effective planning, data and information management practices and procedures can be developed to minimize and manage these risks. Waiting to take action until a subpoena arrives or a dispute erupts is too little action too late.

Document retention involves non-dispute related considerations as well. Corporations often want to preserve ready access to electronic data for sound business purposes. Planning to preserve electronic information and data in the event of a natural disaster or a man made problem can insure the availability or recovery of valuable information. Also, management may be required under federal or state law to maintain information, *i.e.* to maintain corporate records for particular purposes for some period of time. For example, the Sarbanes-Oxley Act of 2002 imposes criminal and civil liabilities which could be implicated for the destruction, mutilation or concealment of electronic data which obstructs or impedes an official proceeding. These needs must often be met while controlling the amount and thus the cost of data stored with the respective benefit. In addition, and most importantly, all persons involved should be mindful that data and information must also be preserved where it relates to reasonably foreseeable civil or criminal litigation (whether involved as litigant or a third party) or a governmental agency investigation, *i.e.* an investigation by OSHA, the Justice Department or a state Attorney General.

Once the duty to preserve information arises, corporate management must affirmatively act to preserve relevant records and/or data that they know, or should within reason know, are relevant might lead to the discovery of admissible evidence, or that are the subject of a discovery request.

This obligation is nearly the same throughout the country. The United States Court of Appeals for the Fourth Circuit has held that "[t]he duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation." *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001). The willful destruction of evidence or the failure to preserve potential evidence in a pending or future litigation is called "spoliation" by the courts.

Courts are increasingly inclined to hold corporations accountable for spoliation. The punishment handed down for spoliation can be severe. In 2004, a federal judge punished a company for deleting relevant emails by deciding to instruct jury during the trial that the contents of the emails would have been favorable to the party deprived of the emails. The same judge forced the party who wrongly deleted the emails pay for the cost of additional depositions and re-depositions. *Zubalake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. 2004). In addition, failure to properly manage electronic documents can produce increased litigation costs, regulatory penalties and court imposed sanctions. A corporation will not be excused from the duty to preserve electronic evidence merely because of its own size or the attendant expense or complexity of compliance.

Advanced adequate preparation is the answer. Data may be stored in differing locations, including networks, lap tops, compact discs, floppy discs, back up tapes, home computers, hard drives, etc. The sheer multitude of places where electronic information may be stored or resides requires the development of a sound action plan. An effective plan must be developed and executed prior to a dispute or a government investigation.

Every company should consider how it will discharge its preservation duties before the occasion arises. To avoid confusion or half measures, reasonable written policies and procedures should be prepared, adopted and followed. These policies and procedures must be practical and reasonable. Unless some legal duty requires an organization to keep electronic information, the systematic destruction of electronic information is perfectly fine and defensible. In this regard, electronic documents and paper documents are similar.

Every organization should first assess its own needs in connection with retaining and discarding data. This exercise ought to involve considering operational needs, existing technological infrastructure and disaster recovery plans. Then the organization should formulate understandable document retention and preservation policies which should be updated from time to time to consider new technologies, business matters or regulatory requirements.

At a minimum, a company's document retention and preservation policy should outline the affirmative steps that must be undertaken when a duty to preserve electronic information becomes apparent. This involves notifying all employees likely to have relevant information in their possession or control that such information must be preserved when a duty arises. At the

same time, employees must be instructed to cease the deletion or destruction of any and all relevant electronic records. This is sometimes referred to as a "litigation hold." Management must communicate these instructions clearly, forcefully and promptly. All efforts to suspend document destruction and commence preservation should be documented by management. Documenting these actions, particularly if they are systematic and reasonable, could help mitigate problems if some inadvertent deletions occur. Toward that end, every employee at every level should understand that management expects all employees to fully and faithfully comply with its policies.

Improper document destruction is a bell that cannot be unrung. An information management plan is not a ministerial function that should be delegated to the person who updates the software or troubleshoots technical problems. A plan which rests upon prompt and effective action is necessary to minimize risk. This may be more easily accomplished by designating a person or persons with the authority and the obligation to put electronic document destruction policies on "hold." Ideally, an organization would train employees in advance about its expectations with respect to the obligations of individual employees.

There is no "one size fits all" approach that will satisfy the needs of every company. The president of a small business contractor with a single computer network and a few employees with Palm Pilots may well develop a simple yet highly effective document management policy that would be wholly inappropriate for a larger contractor. On the other hand, a large contractor might ideally require input from executive management, employees involved in information technology, the outside auditor and legal counsel to develop a policy regarding the means and methods for retention and preservation of electronic information. Sound planning and adequate preparation can insure the availability of necessary historical electronic information, assure a cost effective utilization of information storage capacity and prevent expensive, problematic issues when disputes arise, litigation occurs or governmental investigations commence.