

Information Management in an Electronic Age

By: John P. Sieminski, Esquire
Burns, White & Hickton, LLC

Information Explosion

The world is going digital and the business world is no exception. It is estimated that over 90% of new information is created on an electronic device in digital form. Of that electronic information, it is also estimated that approximately 30% is created, used, maintained, stored or destroyed without ever being printed to paper. The construction industry is no exception to this trend. The industry has embraced the use and exchange of information that, fifty years ago, would invariably have been created and used in the traditional form of paper drawings, specifications, letters, memos, and other traditional forms. For the reasons discussed below, electronic mail is a form of digital information that has achieved particular prominence and deserves special attention. In addition, the sheer volume of information created in business and non-business settings is staggering. Researchers at the University of California at Berkeley estimated, for the year 2003, that five exabytes of new information were created and that the amount of new information is growing each year. (One exabyte is 1,000,000,000,000,000,000 bytes OR 10^{18} bytes.)

Recent Cases Involving Electronic Documents

The move to doing business electronically has created interesting twists on traditional exposures and has created unique and significant liabilities for business organizations of all sizes. Courts are extending common law duties requiring the retention of information relevant to ongoing (or reasonably anticipated) litigation to information in electronic form. Applying the doctrine of "spoliation," courts across the country have consistently imposed sanctions on business who have failed to have their electronic information houses in order. The dollar value of the sanctions has often been enormous.

In perhaps the most-cited case, *Zubulake v. UBS Warburg*, a federal district court jury in New York awarded the plaintiff, Laura Zubulake \$9.1 million in an employment discrimination matter. In what most observers agree would have been a routine employment case, the parties became embroiled in a protracted dispute about electronic data, mostly e-mails, that became critical to the result. The presiding judge issued a series of opinions that set forth a number of guiding principles in what has become known as "electronic discovery." In essence, the electronic discovery dispute centered on an allegation by the plaintiff, Ms.

Zubulake, that certain e-mail communications by her managers contained evidence of the gender bias that she sought to establish as her primary claim.

After extensive discovery proceedings involving the existence and location of the allegedly discriminatory e-mails, it became apparent to the Court that UBS Warburg had failed to diligently seek and insure the preservation of all of the e-mail communications that might be relevant to Ms. Zubulake's claim. Upon review of the haphazard manner in which UBS Warburg approached the discovery process, the Court determined that UBS Warburg had not properly instituted and enforced a "litigation hold" preventing the destruction of potentially relevant electronic material. As a sanction, the Court at trial gave an adverse inference instruction to the jury, essentially advising it of UBS Warburg's electronic discovery transgressions and allowing the jury to assume that, had the relevant e-mails been produced, they would have impacted negatively on UBS Warburg's defenses.

More recently, the case of *Coleman v. Morgan Stanley* garnered considerable attention by the business and even the popular press. Financier Ron Perelman sued Morgan Stanley for fraud in connection with his sale of stock in Coleman to Sunbeam. A state court in Florida awarded Mr. Perelman \$604.3 million in compensatory damages. More remarkably, however, the jury added \$850 million in punitive damages to its verdict upon a finding that Morgan Stanley had not engaged in the electronic discovery process in good faith. This portion of the verdict was based primarily on a certification by Morgan Stanley that all relevant electronic information had been produced, when, in fact, a subsequent and significant volume of information was later discovered.

The litigation hold requirement is not applicable to just the financial or public sectors and has been applied to enterprises across the business spectrum. Any organization that anticipates, or reasonably should anticipate, litigation is required to take reasonable measures to preclude the destruction or disposal of electronic information that may be relevant to the matter.

Practical Effect on the Construction Industry

Of what relevance are these cases to architects, engineers, contractors, and other participants in the construction industry? Courts are imposing "litigation hold" duties on organizations who in are involved in, or who reasonably anticipate, litigation, regulatory investigations, or valid third-party requests for information such as subpoenas requiring the production of documents. In respect of the sometimes adverse and litigious nature of construction projects, construction industry participants should have policies in place to prevent the destruction of information, whether it is electronic or paper, that may be relevant to a dispute.

On the other end of the preservation-destruction continuum, the proliferation of information of all types presents challenges in the management, storage, and ultimate destruction of documents, both electronic and paper. There are good business reasons, recognized by courts, for regular identification and destruction or disposal of information that no longer serves a useful business purpose. The United States Supreme Court, in a case involving the demise of the Arthur Andersen accounting firm, recently recognized the validity of disposal of information pursuant to an appropriate document retention policy.

A corollary issue that arises in the absence of appropriate destruction pursuant to a defensible information management policy is the lost revenue associated with the time it takes, in both litigation and business settings, to handle information that could have been disposed of or destroyed. As anyone who has been involved in the discovery process in almost any construction-related dispute can attest, the soft cost of combing the project record for documents that a party is required to produce, or which may affirmatively be used by a party to assert its claims or defenses, is considerable. Given that, for example, the material on a half-full forty gigabyte hard drive, when printed to paper, might fill a file cabinet, it becomes apparent that document retention policies must be applied with equal vigor to both paper and electronic documents.

Electronic Mail: A Special Form of Electronic Document

E-mail is a form of electronic information that bears special scrutiny. It is estimated that over 80% of all business correspondence now takes the form of electronic mail. Like other forms of electronic documents, there are significant differences between e-mail and traditional paper that pose particular challenges. The speed with which e-mail can be sent and forwarded to hundreds or even thousands of recipients makes the process of printing paper correspondence, copying it, and stuffing it into envelopes to be deposited in a mail chute seem glacially slow in comparison. In addition, automatic copying and retention by electronic mail programs, ordinary backup procedures, and the retention habits of senders and recipients sometimes make the notion that any given e-mail message can be destroyed seem futile. Finally, like other forms of electronic documents, the digital information contained in e-mail is susceptible to being tampered with or changed by relatively unsophisticated users who have nefarious motives.

There is another troublesome aspect of e-mail that is not necessarily a function of the technology that produces it. There is perception of informality associated with e-mail that causes many users to include statements that they would never think to include in more formal correspondence such as memoranda or letters. Legal publications are replete with cases in which users of e-mail have sent messages containing clear and unequivocal evidence of negligent, criminal, or

otherwise inappropriate behavior. Companies have also been exposed to civil liability as the providers of e-mail and other types of computer systems used inappropriately even though the use was clearly not related to the business carried out by the organization.

The Need for an Information Management Policy

Construction industry participants were, of course, early embracers of technology in the guise of the project web site, on which the communications process attendant to design and construction of a project is carried out in electronic form. The cases and concepts described above make it clear that it is incumbent upon all business enterprises to manage the creation, use, and destruction of information in all forms. A comprehensive information management policy should include components setting forth the manner in which information may be created, obtained and used (i.e. a content-driven acceptable use policy) and the manner in which it should be retained, stored, and ultimately deleted or destroyed (i.e. a document retention policy). Experience has taught that there is no "one size fits all" policy: Information use is industry-specific and organizations within the same industry use and maintain information in different ways. Policies must therefore be tailored to fit the requirements and culture of each business organization.

Architects and other design professionals, for example, may be required to retain design documents for certain statutorily-mandated periods. It is incumbent upon contractors to retain documents pertaining to payroll and workers compensation coverage for appropriate periods. All businesses are subject to federal requirements pertaining to the retention of certain human resources documents. Additionally, all organizations must manage the enterprise-specific tension between the desire to retain relevant and useful information and the cost and waste associated with retaining large amounts of information that no longer serves any useful purpose.

Small organizations often believe that they are too small to be affected by these issues, but that is a short-sighted view. The multi-million dollar liabilities incurred by large organizations are easily scalable to smaller enterprises with a concomitantly less dollar value but similarly catastrophic effect on the bottom line. In addition, the cost of preparing a defensible information management policy can often be dwarfed by the consequences of failing to have one, a concept that also applies to organizations of all sizes. Finally, creation and adoption of a policy can constitute a complete waste of corporate time unless upper management supports the policy and it is regularly applied, enforced, and compliance is audited.