Documents, Bad Documents, and Worse Documents: Retaining and Destroying Documents and Data and the Effect of Litigation

By Andrew R. Lee[1]

Introduction

The "document retention policy" has been a fixture of the business world for decades. In simple terms, such internal policies instruct employees on what documents to preserve and what ones to destroy. But the policies of 30 and even ten years ago are becoming less functional in the digital age, when the concept of a business correspondence "document" has a significantly different meaning from that of even only a few years ago. In fact, a recent study concluded that 93 percent of all "documents" now originate in an electronic format. As significant as the fact that only 7 out of 100 business documents do not originate in some form of computer mechanism, the vast majority (70 percent) of the digitally-created 93 percent of business documents never make it to paper, and many of those remain on company computers indefinitely.

This phenomenon of "perpetual documents" can and does have serious consequences. Companies that do not have document and data retention policies and programs that actively destroy "dated" electronic data could experience severe corporate heartburn *when* (not *if*) they become embroiled in litigation. Indeed, as soon as litigation is imminent, those 93 out of 100 documents are required to be preserved indefinitely and are subject to "discovery" and production to an adverse party, in many cases even if they are not specifically requested.

It should be clear why the business community should care about the proliferation of perpetual "e-documents" in the digital age: in those "e-documents" the litigation adversary is likely to find a goldmine of information – or possibly the single "e-nugget" that may be the ticket to a large jury award. Recent court decisions have caused the corporate community to take notice of the challenge of dealing with archiving, retaining, and destroying "hardcopy" and electronic data in a reasonable and organized manner. Failure to focus on the problem is unwise, as the challenge of a workable retention policy will only prove more difficult as record collections multiply and as new communication methods such as digitized voice mail – a medium that is potentially as permanent and accessible as e-mail – come online.

While widespread destruction may appear to many businesses to be the favored option, these entities actually are faced with a dilemma – retain too much electronic data and risk incurring exorbitant costs in producing that information in litigation, or retain too little data and risk being sanctioned by the courts for spoliation of evidence, or, possibly worse, throwing out the "good with the bad" – the favorable evidence is lost along with the unfavorable material. Faced with the risk of sanctions for failing to preserve documents, and of adverse lawsuit damage awards for keeping "bad documents" beyond what the law requires, it is imperative that companies address document and data retention long before any litigation discovery process begins.

Document Retention and Destruction: Reasons for Implementing a Written Records Management Program

Whomever is responsible for the old adage, *"if it ain't broke, don't fix it"* must not have been familiar with the concept of "archived file storage," not to mention hidden

computer “metadata,” e-mail “PST” files, or instant messaging. Indeed, most business leaders will not have an idea of how “broke” their companies are until they are in the thick of a litigation battle in which “smoking gun” documents are found and used to the target company’s detriment. These “voices from the grave” can take the form of paper memoranda or, in the modern age, more likely will haunt companies from the “ether” when they are recovered from computer and network hard drives, PDA’s, personal laptops, and even cellular phones.

Companies that operate without a comprehensive, workable records retention and management policy, or do not consider having such a policy to be a priority, should consider the ramifications of such a position:

- Is it conceivable that the company could be sued by a disgruntled stockholder, executive, or employee, a competitor, a supplier, or a regulatory body?
- If the company were to be sued tomorrow, what assurances do its executives have that key documentary evidence supportive of the company’s position remains available?
- If a regulatory body were to commence an investigation against the company, is the company in a position to communicate to the agency what documents and data and are not available and the protocol whereby the company has destroyed the unavailable documents??
- If certain documents / data have been destroyed, could the company produce a written and broadly-implemented and executed records

management policy that would support the prior destruction of the missing material?

"Horror stories" abound that illustrate well the folly of ignoring the need for a "document retention and destruction" or a "records management" program or policy in any business environment where records are kept and maintained, where legal and regulatory concerns exist at any level. The concept has gained prominence in the modern, "wired" commercial environment of the early 21st Century, and it implicates nearly every type and size of business. Indeed, the consequences of a company's operating without an effective records retention and management program (that is followed) are almost always negative. Storing unneeded archives – whether paper or electronic – can be expensive, but these costs pale in contrast to the sanctions that can be imposed on businesses both in civil litigation and in the regulatory context where a working document retention policy does not exist or is gathering dust.

A Records Management Program is a process whereby the company deliberately designates the records that it will maintain, the period of time for maintenance of such records, and the procedure for their destruction. The goals of such a program are to retain only those documents that are necessary to comply with the law and that benefit the company (and for only that long), and to maintain securely the materials that must be kept for legitimate reasons.

An effective records management program should accomplish the following:

- Identifies those documents that must be maintained in accordance with the law;

- Identifies those documents that the business must keep to effectively function;
- Tracks the company's maintenance efforts;
- Lays out a schedule for the systematic destruction of records in accordance with the above guidelines;
- Effectively destroys the documents that are scheduled for elimination under the program; and
- Monitors and audits the company's execution of the program.

What Should You Be Doing Now?

Often, companies find themselves in a bind when litigation arises because they have failed to adequately address electronic data retention and destruction. Companies often do not know what electronic data they actually have, which can cause major problems. In order to adequately prepare for future litigation, companies must have a clear understanding of exactly what electronic data they have on hand that is easily accessible and, therefore, must be produced to the adversary at the producing party's cost, if and when litigation arises. Companies also must understand that electronic data stored on backup tapes or other inaccessible media may take significant time and money to retrieve and review. If a company keeps this material, it may be required to produce it at a hefty price, as expensive experts are often required to retrieve data from antiquated or obsolete systems. Knowing what you have will aid you in devising (or updating) an appropriate retention policy and will help you respond timely and adequately when faced with a request for electronic data in litigation or otherwise.

Companies also find themselves in hot water when litigation arises because they do not have data retention policies or they do not monitor and revise those policies as time goes by. Companies should have a specific data retention policy that dictates when, how, and how often, electronic data is backed-up and later purged. This policy also should set forth specific procedures for notifying the party in charge of the system when litigation seems likely, so policy implementation can be modified to avoid inadvertent destruction of potentially-relevant information. Controls should be put in place to provide notice of the need to retain electronic data prior to or at the start of litigation. Companies must take action to make sure that their employees are actually abiding by the data retention policy, so that they are not caught off guard when faced with litigation. Simply having a policy in place is not enough; you must ensure that it works and that your employees are following it.

How Retention of Documents Affects Disputes and Litigation: Recent Decisions Highlight the Mission-Critical Issue of Document Retention

As of just two years ago, one in every seven American companies has received a court or agency order to produce email.[2] In the highly-litigious business environment of the 21st Century, businesses must be aware of the consequences of mishandling electronic documents. Two critical terms that must be in the lexicon of every executive concerned with business protection measures are "preservation" and "spoliation." Failure to *preserve* or otherwise mismanaging key materials ("spoliation") can result in significant sanctions, including an "adverse instruction" to a trial jury that the business should effectively be punished for its failure to preserve key documents in the context of a court case.

It is not uncommon that businesses on the low side of a bruising litigation battle later regret that certain e-mails or other electronic or paper documents were not destroyed before the trial jury got to see them. However, a litigant who attempts to destroy relevant materials, whether in electronic or paper form, can find itself in deeper trouble than had it kept the damaging document around. Specifically, such parties that fail to preserve relevant documents and data upon the threat of litigation may stand guilty of *spoliation*. This term refers to intentionally or negligently destroying documents or data that is relevant to anticipated or actual litigation or a regulatory investigation. Courts and regulators have granted severe sanctions against parties for spoliation of both paper documents and electronic data.

The dangers of spoliation are especially prevalent where the business does not have a formal policy of document and data destruction that has been consistently implemented and followed. Even where such a policy is in place, if the destruction is not called for by the time that the lawsuit commences, the document must be kept – and ultimately produced to the adverse party.

Several recent cases highlight the point that document and e-data *preservation* procedures must be put in place immediately at the outset of litigation, and they must be monitored regularly, for instance:

- In *Linnen v. A. H. Robins Co.*, sanctions were imposed on the defendant for its poorly implemented record retention policy, and its failure to preserve documents relevant to the litigation. In addition to a monetary costs award, the court issued an "adverse inference instruction" to the jury

that cast an unfavorable light on the defendant for its negligent destruction of e-data.[3]

- In 2004 Philip Morris USA was fined $2.75 million for destroying more than two years' worth of e-mail messages related to the federal government's lawsuit against the tobacco industry. The judge who issued the sanctions said that the stiff fine reflected "the reckless disregard and gross indifference" displayed by the company in destroying the records.[4]

In the regulatory context, the monetary sanctions have been even heavier:

- In February 2005 New York Stock Exchange investigators fined JP Morgan Securities $2.1 million for failing to keep e-mail records as guidelines required.[5]
- In May 2002, a Wall Street brokerage house paid $100 million to settle a New York Attorney General investigation related to the activities of its research analyst group after investigators scoured thousands of e-mails and uncovered correspondence where the analysts contradicted their public stock ratings.[6]
- In October 2002, several Wall Street firms were fined a total of nearly $10 million for failing to maintain e-mail records as required by law. Ironically, the firms argued to reporters that retaining e-mails was "too expensive."[7]

Hold It Right There: the "Litigation Hold"

When litigation is "reasonably anticipated," routine e-mail and e-document destruction is required to cease. While lawyers quibble over the phrase "reasonable

anticipation of litigation" that is often used in this context, there is no doubt that the "litigation hold" must be taken seriously and emphasized to all of the company's involved employees when a lawsuit commences.

Accordingly, when litigation arises or appears reasonably likely to occur, consider the electronic data requests you may confront in the matter and other electronic discovery issues that may arise. It is critical to put your attorney in touch with your IT department early, so that they may collectively plan for and coordinate on electronic data issues. Discussing electronic discovery issues internally and with your attorney early will help you to devise an appropriate budget and strategy for e-discovery. And, more importantly, it can help you avoid harsh penalties in litigation relating to document destruction.

The ABCs of Document Retention Begin With "Z", as in, Zubulake

Several recent decisions involving companies that have failed to observe a "litigation hold" have shaken the business world. In the first half of 2005 juries in New York and in Florida awarded nearly *a billion dollars* in punitive damages against defendants who stood accused of destroying or mishandling electronic data central to the evidentiary core of those cases. In both instances, the judges intervened to sanction the defendant companies for their failure to produce – or to produce timely – e-mails and other data that the plaintiffs requested. The cases are widely viewed as roadmaps to litigants and counsel at the outset of litigation to preserve the "electronic paper trail" of e-mails, word-processing documents, databases, spreadsheets, and other data that has replaced paper in the business world, or face a severe alternative that could result in a large adverse court award.

The cases of *Zubulake v. UBS Warburg*[8] and *Perelman v. Morgan Stanley* chronicle what happens to a corporate defendant that ignores its duties to preserve and produce electronic discovery. In the first case, decided in April 2005, a New York jury awarded $29.2 million to Laura Zubulake, an investment trader who claimed that her former employer, UBS Warburg, had discriminated against her and ultimately fired her because of her gender. The court decision followed a judge's pretrial ruling that:

- several UBS Warburg employees failed to heed its counsel's repeated instructions to *preserve* e-mails; and
- UBS Warburg's counsel failed to *monitor* the client's compliance with the directive, which the court said compounded the data loss.

The pretrial decision, labeled *Zubulake V* because it followed a succession of "e-discovery" rulings in the case, awarded attorney's fees and recovery of costs to the plaintiff. But these monetary sanctions were the least of UBS Warburg's worries, as the court also decided that a crippling "adverse inference" instruction would be read to the jury at trial. The instruction allowed the fact-finders to *infer* that the destroyed e-mails contained evidence harmful to UBS. The large $20 million punitive damages component of the jury award has led many to conclude that the jury intended to punish the investment bank defendant for its negligent and bad-faith handling of e-mails in the early stages of the litigation.

In May 2005, a south Florida courtroom was the setting for another "e-discovery" fight that resulted in a massive jury award. There, the Morgan Stanley investment bank was the target of a securities fraud claim brought by billionaire financier and Revlon chairman Ron Perelman, who claimed that Morgan Stanley helped Sunbeam Corp.

conceal accounting problems that significantly reduced Perelman's investment in the appliance maker. What most hurt Morgan Stanley, however, was its own alleged mishandling of e-mails, some of them over five years old. A month prior to trial, Florida Circuit Court Judge Elizabeth Maass found that Morgan Stanley had been "grossly negligent" in producing the e-mails and other electronic documents relevant to the dispute and also heaped blame on the company's outside counsel. While Judge Maass also issued an *adverse inference* instruction, she did *Zubulake* Judge Schira Scheindlin one extreme better when she effectively reversed the burden of proof from Perelman to Morgan Stanley by telling the Florida jurors that they could infer that Morgan Stanley had helped Sunbeam defraud Perelman. Unable to carry this extreme burden, Morgan Stanley suffered a resounding loss as the jury awarded Perelman $604 million in compensatory and $850 million in punitive damages.[9]

These decisions are part of a trend showing a higher level of sophistication among trial judges who are now questioning litigants' claims that they cannot locate and preserve the e-mails and other data that may be relevant to a dispute. The cases also portend that courts will have little tolerance for parties and their counsel who fail to grasp the relevance of electronic records, including e-mail, in litigation. Finally, as did the judges in both cases, courts are apt to reject incompetence or routine destruction of bits and bytes as excuses and instead may rule that parties' noncompliance is an indication that they have something damaging to hide.

Is Help On the Way?
New Civil Discovery Procedural Rules
Show Promise

New civil litigation discovery rules appear to favor corporations whose business may depend upon the ability to recycle backup tapes and to keep in place other regular document retention (and destruction) practices. One of these new rules, which went into effect in December 2006, will attempt to distinguish between data that is "readily accessible" and electronic material that is more difficult to restore from archived backups.[10]

Whether an electronic-data request is unduly burdensome or expensive depends primarily on how each party maintains its data. Data that is currently available is considered accessible and relatively inexpensive to produce, so the producing party should bear that cost. Deleted data, data contained on backup tapes, and data stored on antiquated computer systems is considered inaccessible, and thus may be unduly burdensome or expensive to produce. Inherently inaccessible data may warrant cost shifting. Currently, courts apply various tests to determine whether or not cost shifting is appropriate; there is no uniform rule for making such a decision.[11]

The new rule, however, places the cost burden of electronic discovery of "accessible" data on the responding party. Access to "inaccessible data," however, requires the responding party to pay the costs associated with its restoration to "accessible" form.[12] This rule codifies that businesses will have to spend money to accommodate adverse parties in litigation seeking information on archives such as backup tapes, and that the cost burden associated with this should be borne by the requesting party. Meanwhile, plaintiffs' lawyers have balked at the "inaccessible /

accessible" distinction, arguing that "[p]arties resisting discovery shouldn't be relieved of the obligation to demonstrate undue burden simply because evidence resides on a backup tape."[13]

The rules will reward the business that has a working document retention policy – one that is being followed by the company's employees – in place when litigation ensues. In a litigious society where communications in the form of e-mail many times form the evidentiary framework of a litigated dispute, every company – regardless of its size – must consider a document retention policy in its business plan.

These rules also require parties to discuss the form of production of electronic data, retention and preservation of such data, and privilege waiver issues at their initial discovery conference, which typically occurs very early in litigation.[14] The purpose for this change is to reduce (and possibly eliminate) problems that might otherwise arise later in litigation by requiring thoughtful attention to document retention and e-discovery at the outset of a case.

Along the same lines, the new guidelines expand parties' initial disclosure requirements to include information regarding each party's electronic data storage systems and electronic communications systems.[15] This will force all parties to address what electronic data they have and how they maintain it.

The proposal also introduces a rule setting forth a data preservation protocol that provides parties with guidance and certain assurances regarding their data retention practices.[16] This rule rewards the company that has a working document retention program in place. An additional benefit is that the provision eliminates much of the guesswork currently surrounding the adequacy of data retention when litigation arises.

What Can You Do Now?
Tips for Easing the Pain of E-Discovery

The changes to the discovery rules are aimed at eliminating inconsistencies among courts in dealing with electronic discovery issues. Moreover, they should take much of the guesswork out of electronic discovery matters for litigants. These new rules augur for additional precautions that, some would say, accomplish the ultimate goals of the new rules.

1. **Discuss Electronic Discovery Issues at the Start of Litigation**. When litigation starts, consider the electronic data requests you may confront in the case and other electronic discovery issues that may arise. Put your attorney in touch with your IT department early, so they can plan for and coordinate on electronic data issues. Discussing electronic discovery issues internally and with your attorney early will help you to devise an appropriate budget and strategy. And, it will help you avoid a *Zubulake* situation.

2. **Contact the Opposing Party to Discuss Electronic Discovery.** Discuss electronic discovery issues with the opposing party at the early stages of litigation. Trade information regarding your electronic data storage systems, your data retention policies, and your expectations regarding electronic discovery in each particular case. Additionally, discuss your expectations regarding the form in which requested data should be produced, address privilege waiver issues, and consider entering into a joint stipulation preventing inadvertent privilege waiver, in the event that

an otherwise privileged document is inadvertently produced as part of voluminous e-discovery. Coupled with the protections afforded under Rule 26(b)(5)(B), such a stipulation can ease the burden and delay often associated with reviewing electronic data prior to its production.

3. **Be Creative.** Consider how you can work with your opposing party on ways to lessen the burden (both time and money) of electronic discovery. For example, if your adversary requests information contained on voluminous backup tapes or on other inaccessible media, suggest that you conduct an initial review of a random sampling of such data to determine how much, if any, relevant information might be contained on the back up tapes. The results of such a sampling will help you to determine the relative utility of restoring and reviewing the full extent of the otherwise inaccessible data. Be open to unique solutions to discovery-related problems tailored to the facts and circumstances of each case.

A Bigger Problem: A Workable e-Data Retention Policy; Guidelines for Document Destruction

Less than 40 percent of respondents to one 2004 poll said that their organizations trained their employees on records and information management issues.[17] This statistic refers to "paper" document retention policies. Recent studies indicate that the lack of direction is even more compelling in the realm of electronic information. One such study indicates that more than 60 percent of companies have no method available to them to apply a litigation hold to electronic records when pending litigation requires it.[18]

In order for electronic document retention programs to work, companies will have to adopt solutions that either (a) require end users to manually classify records according to company- or department-defined file plans, or (b) automate this process through the use of automatic metadata labeling or e-mail categorization. Experience has proven that users will not follow a process that is manual in nature, so automated software solutions will have to address this area of need. Such solutions revolve around automatically training the software program to recognize categories of documents based upon content. In the case of e-mails, the sender-receiver information and other objective data serve to automate categorization.

In a world in which e-mail has replaced written correspondence and electronic documents have replaced "paper" versions, fashioning a "document retention policy" that addresses electronic data is a significant challenge. Doing so involves multiple considerations including:

- **Separating the "good" from the "bad":** Unlike a paper record, whose "universe" of information is contained within the document's "four corners," electronic records typically exist in several components, which are located on different computers in different locations. Thus, it is important with an electronic record to ensure that what you have and what you produce is the entire document and not merely a portion of it. This becomes difficult to manage when dealing with e-mail trails between multiple parties and circulated attachments. Additionally, electronic documents, by their very nature, are easier to alter than paper records; accordingly, proper controls must be in place to avoid alteration or

destruction of electronic documents. The reliability and integrity of an electronic document can be key in litigation, as those qualities will affect the admissibility of the documents in a court proceeding.

- **Multiple locations and media.** Just about everything purchased within the last five years has a processor. Handheld, laptop, and even mobile phones may contain copies of files and e-mails subject to deletion. If a company policy requires deletion based upon information dating, it must also take control over rogue copies that may exist on these often overlooked media.
- **For everything there is a season.** How long each company – or even division or department – keeps documents and electronic data depends upon legal requirements unique to each such division or department. In many cases, specific statutes prescribe the time periods. Coordinating the document retention policy to square with varying legal requirements will likely require a lawyer's assistance.
- **How to destroy the indestructible?** When does hitting the "delete" key really cause a file or e-mail to be trashed? An e-mail recipient who presses "delete" to rid a system of an e-mail does nothing to the version on the sender's side, of course. But the difficulty does not end there. If the data resides on the system server, system-wide processes must be in place to ensure deletion occurs via data "overwrite." That is, deleted data remains in a computer's memory until it is overwritten by new data. If a company does not specifically employ a data "overwrite," deleted data

will remain available (and discoverable) long after the stroke of the delete button.

- **The business exists to make widgets.** Companies install computer systems to serve the company's executives and employees, not the other way around. The retention policy must be written with the business of the company in mind. The retention policy author must find ways to ensure that restrictions on data retention and destruction do not restrain business.

Without a Document Retention Policy That Works, All the "Bad" Documents Are Left Behind

It would be nice to retain only "good" documents, with "bad" documents instantly designated for the "Trash" bin. Nice, but simply not possible. Even were such a mechanism available, soothsayers would have to be retained to somehow determine in advance whether a document or e-mail will prove "good" or "bad" in the context of litigation. Realistically, only retention policies that are based on "neutral" principles will withstand scrutiny in a lawsuit.

As a result, policies must include a "preventative medicine" component, that is, to protect itself from liability in litigation, companies should include in their e-document retention policies a strong instruction that *software, and particularly e-mail, is for business use only*. Likewise, employee computer software training and orientation should emphasize that the "golden rule" applies to e-mail usage: *don't put into an electronic message what you wouldn't want your spouse, mother, or children to read*.

Conclusion

The above lessons have broad application. In the 21st Century business climate, companies are not asking the question "whether" they will see the inside of a courtroom some day, but "when." Planning for electronic data preservation, as well as reasonable retention and destruction practices, is becoming less optional and more of a mandate than ever before.

---

[1] **Andrew R. Lee** is a partner in the New Orleans office of Jones, Walker, Waechter, Poitevent, Carrère & Denègre, LLP. Mr. Lee received his B.A. from Tulane University and his J.D. from Washington & Lee University, and is listed in the 2004-2007 editions of *Best Lawyers in America*. His e-mail address is alee@joneswalker.com.

[2] G. Keizer, "Lack of E-Mail Policies Could Put Companies in Hot Water," INFORMATIONWEEK, June 17, 2003, http://www.informationweek.com/story/showArticle.jhtml?articleID=10700336 (visited August 8, 2005).

[3] No. 97-2307, 1999 WL 462015 (Mass. Super. June 16, 1999).

[4] "Judge Fines Philip Morris for E-Mail Loss," New York Times, July 22, 2004, C1.

[5] "J. P. Morgan Chase Unit is Fined Over Record-Keeping," New York Times, Feb. 15, 2005, C1.

[6] "Power Struggle May Hasten Transition at Merrill Lynch," New York Times, June 3, 2002, A1.

[7] R. Smith, "Wall Street Has E-Mail Problems," Wall Street Journal, Aug. 2, 2002, C1.

[8] *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003).

[9] *See* S. Craig, "Jury Sides With Ronald Perelman In Case Against Morgan Stanley," Wall Street Journal, May 16, 2005, A1.

[10] *See* F.R.Civ.P. 26(b)(2)(B)(eff. Dec. 1, 2006).

[11] *See* U.S. Judicial Conference Advisory Committee on Civil Rules, 2004 proposed amendments to Fed. R. Civ. P. 26(f).

[12] *See* U.S. Judicial Conference Advisory Committee on Civil Rules, 2004 proposed amendments to Fed. R. Civ. P. 24(b)(2)(C) and Fed. R. Civ. P. 26(c).

[13] *See, e.g.* G. Paul and B. Nearon, *The Discovery Revolution*; ABA 2006, at 117-18.

[14] *See* U.S. Judicial Conference Advisory Committee on Civil Rules, 2004 proposed amendments to Fed. R. Civ. P. 26(f).

[15] *See* U.S. Judicial Conference Advisory Committee on Civil Rules, 2004 proposed amendments to Fed. R. Civ. P. 26(a)(1).

[16] *See* U.S. Judicial Conference Advisory Committee on Civil Rules, 2004 proposed amendments to Fed. R. Civ. P. 37(f).

[17] AIM International / Kahn Consulting, Survey of 401 End-User Organizations, excerpted in J. Gable, "What's Next for Compliance?", TRANSFORM MAGAZINE, Dec. 2004, at http://www.transformmag.com/showArticle.jhtml?articleID=53200351.

[18] *Id.*, citing 2004 Cohasset Associates survey of 2,200 businesses.