COMPLIANCE WEEK
The leading resource on corporate compliance and governance for U.S. public companies.

Document Creation, Retention, And Destruction Policies

By Harvey L. Pitt, Compliance Week Columnist—Sept. 26 2006

As a practicing lawyer, my clients were all well aware of the infamous "Pitt's Postulate": Whenever you think you've destroyed the last copy of any document, there's always one more that exists, and it will surface at exactly the most inopportune time. The only exception, of course, is if you really need the document, at which point you'll discover that you actually did destroy the very last copy.

As we've moved from hard-copy to digital documentation, the complexities of record keeping have increased exponentially. And prosecutors as well as judges have made it clear that the failure to maintain or produce documents can have dramatically negative consequences.

Sometimes, even intelligent people make bad situations worse. Time and again, when people learn that they or their companies may be the target of a lawsuit or government investigation, they panic and attempt to "clean up" their files, which is often perceived after the fact as a direction to rid one's self of potentially incriminating evidence. The problem, as the English writer G. K. Chesterton observed, "isn't that they can't see the solution. It's that they can't see the problem." Martha Stewart was done in not by the phone log containing a message from her stockbroker evidencing her knowledge of insider trading, but because she altered the message on her assistant's computer and then ordered her assistant to change it back. Former Credit Suisse First Boston investment banker Frank Quattrone's now famous email advising it was "time to clean up those files," was sent after he purportedly learned of a Securities and Exchange Commission investigation, which led to obstruction of justice charges. Arthur Andersen's in-house lawyers sent around a memo reminding the Enron engagement team of the firm's document and retention policy, which—unsurprisingly—led to massive shredding at precisely the wrong time.

Despite appellate reversals in the Andersen and Quattrone convictions (based on problems with jury instructions) it's critical that the lesson in each case not be lost: Improper document retention and destruction practices expose both corporations and their employees to dire consequences. Parties are obligated to preserve evidence that's relevant to current or expected litigation or government investigations.

Eleventh-hour orders to the troops hinting that documents should be destroyed or altered, delivered after a company learns about (or folks within the company anticipate) a government investigation, are a criminal violation under the Sarbanes-Oxley Act, carrying penalties of up to 20 years in prison. Although SOX took effect four years ago, too few companies have taken sufficient measures to ensure that their document retention policies and procedures enable them to produce all subpoenaed records that may be required. The penalties for not producing evidence in a timely and accurate fashion—or worse, being accused of intentionally destroying documents to hamper an investigation or proceeding—can result in multimillion dollar damages and severe reputational damage. The damage done can easily exceed the consequences of underlying fraudulent behavior.

At the same time, the challenges companies face in meeting their compliance obligations during litigation or an investigation are mounting because of the proliferation of emails, instant messages, and other electronic information. In 2003, Peter Lyman and Hal Varian, at the University of California at Berkeley, estimated that, based on the worldwide population, almost 800 megabytes of information is produced per person each year. That's the equivalent of 30 feet of books. According to *The Sedona Principles: Best Practices Recommendation & Principles for Addressing Electronic Document Production*, at least 93 percent of information created is first generated in digital format, 70 percent of corporate records are stored in

electronic format, and 30 percent of electronic information is never printed on paper. Much of this information is "not reasonably accessible," which means that it can't be easily rendered intelligible without great burden or expense.

To alleviate these problems, dramatic revisions to the Federal Rules of Civil Procedure governing the discovery of "electronically stored information," or ESI, are expected to go into effect on Dec. 1. The new rules recognize that the discovery of ESI raises markedly different issues than the discovery of paper records. Under the revised discovery rules, three major changes will occur:

- Litigants will be required to discuss, prior to pretrial conferences, discovery of ESI, and to include this topic in their report to the court.

- Parties will not be required to provide discovery of ESI that's not "reasonably accessible," absent a showing of good cause.

- Judicial sanctions will be prescribed if ESI has been lost or destroyed "in good faith" resulting from routine operation of an electronic information system. However, "good faith" requires that parties intervene to suspend the routine operation of document destruction programs to prevent the loss of information relevant to the litigation.

Although the revised rules reflect a valiant effort to address difficult issues involving electronic discovery, courts are likely to remain quite involved in resolving many issues. In addition, the revised rules will put enormous pressure on companies and their counsel to resolve electronic discovery issues with opposing counsel much earlier in the game.

In light of these developments, there's no better time for companies to revisit the topic of document creation, retention, and destruction. Companies adopting or revamping their policies should keep the following points in mind:

1. **The starting point for all companies is to sensitize employees about when, and how, documents should be created.** If troublesome documents aren't created, most document problems never arise. Employees need to understand when documents should be created, and when they shouldn't. They also need instruction in how to word the documents they do create. The SEC has done much to stamp out "creative accounting," but most companies have done precious little to stamp out "creative memo writing."

2. **Adopt written policies and procedures for managing company information.** Every company needs written policies tailored to its specific operations, structure, and needs to effectively manage its information. Company policies and procedures should deal with ESI as well as paper documents. The object should be to design a program that ensures that information that must be saved, either for business or legal reasons, is retained, while other items are discarded on a routine basis, promptly after they can be discarded under the policy. Effectively managing a company's information and records will make the company's operations more efficient, enabling it to find information that it needs quickly, while ensuring that information and records that should be retained are not inadvertently destroyed. It also will ensure that the company is complying with statutory and regulatory retention obligations and is able to comply with court orders and other litigation obligations.

3. **Document retention schedules.** An integral part of any policy is a schedule that indicates, by document category, how long the company intends to retain documents. Company legal counsel should make certain all statutory and regulatory obligations are met. If the company is in a regulated industry (e.g., broker-dealers, investment advisers, etc.) special rules apply. The policy should explain exactly how the company's document management program will be implemented and what department or personnel will oversee each function, and who can be approached with questions.

4. **Once litigation or an investigation is reasonably anticipated, a "litigation hold" must be put in place.** As the U.S. Supreme Court recognized in the Arthur Andersen case, it isn't wrong for managers to instruct employees to comply with a valid document retention policy under ordinary circumstances. However, once litigation or a government investigation is reasonably foreseeable, the circumstances are no longer "ordinary" and a company must effectively communicate a "preservation

order" or "litigation hold" to appropriate personnel to ensure that potentially relevant evidence is not destroyed, deleted or altered. In addition, to meet "good faith" obligations under the revised federal rules, a company may need to intervene to modify or suspend certain features of their routine computer operations to preserve relevant information. The destruction or alteration of potentially relevant evidence can result in courts imposing crippling monetary sanctions or instructing the jury that an "adverse inference" can be drawn, as well as criminal sanctions under SOX if a government investigation is impeded. In Coleman (Parent) Holdings v. Morgan Stanley & Co., a Florida judge granted the plaintiff's motion for "adverse inference" instructions after Morgan Stanley repeatedly and deliberately was held to have missed electronic document production deadlines and violated discovery orders. The violations included failure to make a good faith search for the oldest backup tapes, failure to notify the plaintiff when additional backup tapes were discovered, overwriting of backup tapes in violation of an SEC regulation applicable to broker-dealers, and belated certifications that were false when made. In May 2005, the jury awarded $1.45 billion in punitive and compensatory damages. Morgan Stanley has filed an appeal.

5. **Policies should contain sanctions for violations of the policy.** The failure to abide by a company's policies should subject employees to appropriate disciplinary sanctions, including possible termination, to be determined in the legal department's sole discretion, whether or not the failure to comply also constitutes a clear violation of law. Employees should be required to certify that they've read and understood the policy and agree to abide by its terms.

6. **Document retention policies must be documented, defensible, and enforced.** Any policy must be able to withstand scrutiny in court and can be used as ammunition in the hands of opposing counsel. In addition, if a company fails to abide by its own policies, it can be certain that can and will be used against it. A document retention policy that isn't consistently enforced is worse than having no policy at all, and having no policy is simply not an option.

7. **Pay attention to document creation, especially emails.** All communications created and distributed by a company's employees, including interoffice memoranda, reflect on a company's reputation and image. Casual or thoughtless messages and off-the-cuff remarks in emails and other electronic communications can have serious legal and financial consequences for both employees and the companies that employ them. The "smoking gun" in many recent cases has been found in emails, and often ones that shouldn't have been written in the first place. If either the employee or the company would be embarrassed to see an email on the front page of The Wall Street Journal, employees should be taught not to write it, send it, or even think it!

8. **Employees should have no expectation of privacy in their emails and companies should reserve the right to monitor them.** Employees often assume their emails are confidential and adopt a casual attitude towards them. Electronic communications and associated files can be widely disseminated well beyond their intended audience. Federal and state regulators routinely make broad requests for emails. Every company should make explicit their right, and intention, to review emails, instant messages and other electronic documents to ensure that the company and its personnel are complying with legal, policy, and practical requirements.

9. **Consider restricting personal communications and participation in instant messaging systems and chat rooms.** Communications by employees during business hours and utilizing the company's communication means should be solely for business purposes. The creation or distribution of any personal, disruptive, or offensive messages should be prohibited, including jokes, games, and chain letters. Employees should also discourage third parties from sending them personal communications or communications with inappropriate content, and should report any communications with inappropriate content to a designated person or department. Finally, while email is an efficient means of doing business, companies should consider prohibiting employee participation in instant messaging systems, posting of information on the Internet, and participation in chat rooms, unless specifically permitted.

10. **Be prepared for Dec. 1.** Companies and attorneys should be prepared in advance of Dec. 1, when the revisions to the federal rules are expected to go into effect. Those who aren't adequately prepared and familiar with their client's data systems (such as accessibility of data, data quantities, locations, types, burdens and costs) won't like the results from their pretrial conferences.

11. **Privilege issues must be carefully considered.** The revised federal rules recognize that, due to the sheer volume of electronic documents, it's difficult to do a full privilege review beforehand. The changes to the rules encourage parties to enter into voluntary agreements providing that inadvertent production of documents does not waive attorney-client privilege. Although the prevalence of these agreements is likely to increase after the new Federal Rules become effective, it isn't clear that these agreements provide protection against waiver claims, and in any event, once a company's internal secrets are revealed, the cat, so to speak, is already out of the bag in the only way that really matters.

12. **Technology can help solve the problems it creates.** We live in a digital age, and the proliferation of emails and other electronic documents makes document management difficult. But technology can also be used to advantage. Excellent software systems are available to help companies create an effective document management system and manage email. Technology can also be used to help search documents for discovery requests. Companies should spend time investigating the various ways that technology can help in this area. The company's IT department and outside advisers can provide much needed help.

13. **Employee training isn't just necessary, it's essential.** In addition to distributing company policies and procedures, companies should hold periodic training sessions so employees are aware of their obligations under the company's information management policies, understand how to meet their obligations, and know who to contact if they have questions. Many serious problems can be avoided if employees understand that all communications they create, send or distribute must conform to appropriate business standards, comply with the law, and not embarrass themselves or the company if made public. In addition, employees need to understand that any violation of the company's policies will lead to sanctions or other remedial action in the company's sole discretion, and that where misconduct violates statutory or regulatory requirements, they can be subjected to criminal and civil liability and broad penalties.

14. **Conduct periodic compliance reviews.** Companies should conduct periodic compliance reviews of their information management policies and systems and take steps to remedy problems they find.

Mark Twain once said he'd been through any number of terrible things in his life, some of which actually happened! Unfortunately, it's predictable that most public companies will be pursued, and many of those will wind up being sued; when that occurs, it's never a happy moment. But with effective document creation and management policies in place, companies can make the best of a bad situation, and avoid making a bad situation even worse.