



Don't Leave An "E-Trail"
The Importance Of An Electronic Document Policy

Unlike shredded or destroyed documents, electronic data isn't always "gone" when it's deleted. You can trash it all you like — even reformat hard drives — but a sharp forensic technologist may still be able to recover the data.

In fact, it has become standard for depositions to commence with an excruciatingly specific examination of a litigant's IT structure, right down to home usage and all computing peripherals, to say nothing of backup procedures and document retention policies.

Conceivably, your firm's electronic "documents" could be in places as far flung as a client e-mail or phone messages, tapes on your personal transcription/tape recorder — even those old computers you've stored away to donate to a local non-profit.

A Concession From The Courts

Recognizing that the sheer volume of a company's electronic documents can be overwhelming, the courts have absolutely accepted the need for data management. In particular, the Zubulake v. USS Warburg opinions have been very helpful in sorting out the confusion.

But while courts have no quarrel with corporations that destroy electronic documents in the regular course of business, the mere scent of spoliation will generally stiffen a judge's resolve to determine whether a company has deliberately destroyed documents. Penalties for spoliation have been severe, including fines, prohibiting the testimony of the person responsible for the spoliation and, in extreme

cases, dismissal of claims.

Get Going

If you or your client do not have an e-document policy, now is the time to begin crafting one — unless, of course, either of you have litigation pending.

There is no one-size-fits-all electronic document retention policy, but the basics are fairly straightforward:

- 1) If you are governed by federal/state law or regulations, follow them. If federal and state requirements conflict, follow the more stringent requirements.
- 2) If you are governed by internal bylaws, other mandatory procedures or industry standards, abide by them.
- 3) If you are on your own after following rules 1 and 2, assume all documents in your possession — paper and electronic — will be the subject of a lawsuit somewhere down the line and act accordingly.

The next step is to determine what electronic data you have and where it is. As you do, you'll need to conduct a thorough analysis, asking:

- 1) Who has access to the data?
- 2) How easily retrievable is it?
- 3) How secure does it need to be?
- 4) How and when can it be destroyed?

Be Ready For Litigation Code Red

Be sure your document retention policy details the circumstances under which the policy should be suspended, such as when a lawsuit is anticipated or in progress, a subpoena has been served or an investigation is known to be underway. Make sure all involved parties know what documents, back-up tapes, etc. must be preserved until the litigation or threat of litigation is resolved. Protect yourself by clearly putting such information in dated writings, whether paper or electronic.

As you begin to formulate a policy, consider who needs to be involved in the drafting — from financial, legal, technical and other departments. If you have outside counsel or an

outside CPA, these individuals will probably also need to be involved. Frequently, an independent electronic discovery consultant is engaged as well.

Our knowledgeable professionals can provide expert guidance and help your firm draft a solid electronic document retention policy that protects your interests as well as those of your clients.