

Electronic Evidence What you don't know can hurt you – a LOT

By Karen Unger

Wrongful termination; tax fraud; trademark infringement; death benefits; breach of contract; personal injury; gender bias: what do these lawsuits have in common?

All had decisions based on electronic evidence. Emails, computer files, and Palm Pilot information all contributed to the final outcome. Electronic documents differ greatly from traditional paper documents to greatly impact today's business.

Recent decisions in lawsuits are significant. Morgan Stanley was fined \$1.45 billion in a case in which email played a significant role. KPMG agreed to pay \$456 million dollars, and opposing counsel asked for sanctions regarding the firm's willful destruction of incriminating electronic evidence.

The Same – Only Different

Hard copy and electronic documents have many similarities. They provide communication between entities. They convey information. They are discoverable in a court of law.

Electronic documents ("E-Docs") are also very different than paper documents. Email and electronic documents have greater volume, are more apt to recreate themselves and just can't seem to be killed. They are dependant on the computers which generated them, but can be shared and searched across

millions of venues quickly. Therein lays both the good news and the bad news.

In 1998, the U.S. post office delivered 1.98 billion pieces of mail. That year, 182.5 billion emails were exchanged. By 2003, the volume of email had increased to 547.5 billion and continues to grow. A company with 100 employees receiving 25 email messages per day generates an estimated 625,000 messages each year. And that's before any emails are forwarded!

The difficulty of dealing with electronic documents is clear.

Persistence

Anyone who watches legal or police television shows knows electronic documents – like the hero in the show – never are really killed. Deleted documents and emails can always be found by the forensic hacker to prove the case.

The delete key removes a pointer to the document's hard drive location, but in fact, it requires hard work, long hours and specialized knowledge to really get rid of a document. File persistence contributes to the complexity of managing documents.

Computer files depend on two things: hardware and software. In order to read a document, a user must have the right application and the right

equipment. However, the internet has created open systems for sharing information across many different platforms. Text messaging and files are shared across computers, Blackberries and PDAs, creating copies in more locations than ever before.

Every electronic document contains semi-hidden information called "metadata." Each file contains an index to determine what application is required to view and process that file. It includes diverse information about the document author, creation date and computer, who last opened and printed it and who made what changes.

Metadata changes every time it is accessed. Opening, copying or printing a document will change vital data. A regular cut-and-paste copy of the document will change the date and location of the metadata. For this reason, care must be taken when preparing documents for use in litigation.

Risk of Spoliation

Spoliation means "the willful destruction of evidence or the failure to preserve potential evidence for another's use in ending or future litigation."¹

1

http://www.ironmountain.com/resources/resource.asp?svc1_code=7&resource_key=1009

Companies can be held accountable for not only the deliberate act of destroying evidence, but also the “failure to preserve.”

In the course of normal business practices, most organizations rotate their back-up tapes. The technology department will have sets of five to seven tapes: Monday’s back-up goes on the “Monday” tape; Tuesday’s on the “Tuesday” tape and so on. The following cycle period, the “Monday” tape is reused by putting the new “Monday” information on that tape. When the possibility of litigation

RESOURCES

A number of resources are available to you in developing effective e-mail policies:

- The Association for Records Managers and Administrators (www.ARMA.org)
- The ePolicy Institute (www.epolicyinstitute.com)
- The American Management Association (*Designing Effective Email Policies* at <http://www.amanet.org> .

arises, organizations start a “litigation hold.” Any document normally destroyed in the normal course of business (retention period has expired; copies are no longer needed) are now required to be kept.

Many times, the technology department either doesn’t get this message or doesn’t think the “hold” applies to backup tapes. But maintaining a company’s standard business back-up practice can be interpreted as “negligent spoliation”. Penalties for this can include fines and attorneys

fees, as well as the inference of wrong doing.²

Consequences

The internet age allows businesses to share documents with greater ease than ever. But every technological improvement is always accompanied by both risk and responsibility.

75% of litigation costs are absorbed by the involved company, either directly or charged back to a business unit, with only 6% being paid for by insurance companies.³ With the sheer volume of electronic documents that abound even in a small company, this can be burdensome.

There are two ways to deal with document threats: defensively and offensively.

Once litigation is pending, several defensive steps must be followed immediately:

- Everyone in the organization must be notified of their responsibilities to preserve evidence.
- Every effort must be made to preserve significant, both hard copy and electronic documents, including:
 - * Email and attachments
 - * Electronic documents
 - * Text messaging
- With legal counsel, determine:

- *How to preserve documents
- *Which documents are pertinent
- *How to make legally defensible “copies” that don’t change the metadata
- Determine who does this work. In most cases, an internal technology department doesn’t have the expertise or time to prepare evidence correctly. Sometimes, it may be more prudent to have a third party perform such tasks.

The real key to protection is proactive planning. Simple steps will take an organization quickly in the right direction before there is litigation:

- Written policies regarding:
 - * Email rights, privacy and ownership
 - * Internet usage
 - * Software downloading
- Document retention policies
- Training for employees regarding policies
- Periodically audits to ensure compliance

Assistance in these matters is available from a variety of sources (see resources sidebar). ***The only choice businesses do NOT have: Ignoring the risk residing in their own computers.***

Karen Unger is president and CEO of American Document Management (www.amdoc.com), which provides litigation support, regional and in-house scanning centers, and hosts retrieval and forms processing for businesses. She can be contacted through her Web site or at 954-462-5400.



²

<http://www.acca.com/chapter/s/program/dallas/accpres081805.pdf>

³ Are We There Yet?; CORPORATE COUNSEL AUGUST 2005