

Lawyers strike e-di



JUST MANAGING LEON GETTLER

MORGAN Stanley's latest email fiasco makes salacious reading. Just two months after it was pinged \$US15 million (\$A20.6 million) by the US Securities and Exchange Commission for failing to retain emails — under the Sarbanes-Oxley law on US corporate governance, public companies are required to retain documents, including email — the investment bank has found itself embroiled in a wrongful dismissal suit in which the plaintiff claims he has emails of X-rated conversations between his boss and an executive director.

The former tech manager also claims to have emails sent by the firm's chief technology officer to put the heat on technology vendors to get top seats at sporting events, and even to give him a go as a Yankees bat boy. Go figure.

Morgan Stanley is now appealing against a \$US1.45 billion award won by financier Ronald Perelman last May. The bank got itself into hot water, partly because it repeatedly botched attempts to produce emails relevant to the suit. Suspecting bad faith or, worse still, an attempt to suppress evidence on Morgan Stanley's part, the judge told the jury to assume the firm had helped defraud Perelman.

Last month, Merrill Lynch was fined \$US2.5 million when it failed to provide the SEC with email messages that the regulators had been chasing for 16 months.

Australian cases featuring electronic documents include HIH, Alpine Offset and Pan Pharmaceuticals. Emails have also figured in the AWB (formerly the Australian Wheat Board) inquiry and in Seven Network's trade practices litigation.

Lawyers say digital forensics, which involves the acquisition and analysis of digital information, and electronic discovery, or e-discovery, are becoming more and more important as legal tools.



And while these are still in their infancy here, trends in the US suggest they are the sleepers that should leave corporate defendants and their in-house counsel very nervous.

For a start, the costs are prohibitive. Under e-discovery, for instance, five folders of photocopied documents can easily turn into 50 folders of emails.

According to one US survey, firms are expected to spend \$US1.9 billion on e-discovery services in 2006.

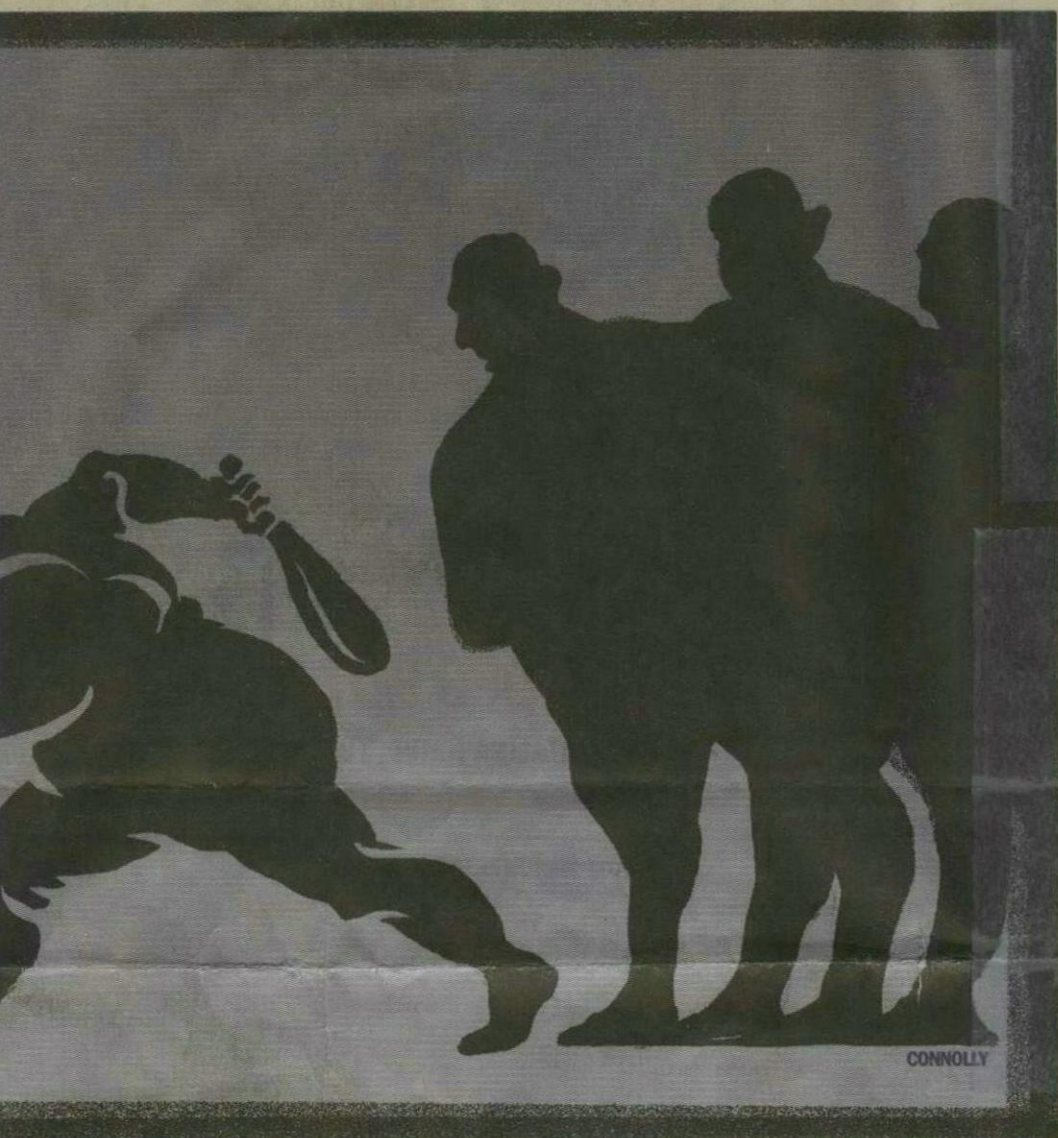
With the cost of finding documents outweighing settlement costs, many companies have opted to settle out of court. The lawyers win both ways and, for a profession renowned for finding new ways of making money, e-discovery is fast becoming a cash cow. David Thompson, managing director of records compliance company AXS-One estimates that 80 per cent of company communication is now handled via email and instant messages.

Potentially, e-discovery captures more than emails, which are usually less carefully worded than other forms of correspondence, are time stamped and are very hard to delete.

Lawyers and document retention specialists claim that it also covers material on office computer hard drives, home computers, personal digital assistants, home computers, laptops, chat room transcripts, data from internet user groups, discs, BlackBerrys, mobile phone records, instant messaging, websites and blogs, phone conference recordings, answer machine and voicemail records and fax machine data.

What makes it particularly dangerous, they say, is that most companies still regard documents as paper. For the record, Federal Court rules define the word "document" to include "any other material data or information stored or recorded by mechanical or electronic means".

discovery jackpot



In Victoria, under the recently passed Document Destruction Bill and by virtue of separate legislation, documents include email.

Under state legislation — introduced in response to the case of lung cancer victim Rolah McCabe against British American Tobacco in which documents were destroyed — due to come into force in September, companies can be fined more than \$300,000 if they are found guilty of destroying documents “reasonably likely” to be used in legal proceedings.

And companies could be found guilty of the crime if the court finds there was a culture that encouraged or tolerated document destruction.

While other states have similar legislation, lawyers say companies are less likely to get penalised under them because those rules are underpinned by common law. With the buck passing and backside covering that can occur in companies it is more difficult under common

law to attribute an offence to an individual as the “directing mind and will” of the business.

The Victorian legislation cuts through this, making companies more accountable. To placate business and guard against a backlash, the Victorian Government set a higher threshold, where document destruction only becomes an offence if it can be proved beyond reasonable doubt that the destroyed documents were “reasonably likely” to be used in litigation.

Lawyers say that what makes electronic documents particularly useful is that they often contain records of who has accessed, modified or printed the document, and the time and date that they did it.

In a paper delivered last month to the Law Institute, technology lawyer and litigator Steve White said that with innovations such as Google Desktop and Microsoft Desktop, companies would find it increasingly difficult to justify

to courts why they have not kept their electronic records up to scratch.

White’s paper argues that conventional backup and purging strategies, and rules governing the use of email would all need to be reviewed as e-discovery and digital forensics become the norm.

He told *The Age* that e-discovery works by detecting key words and patterns, including the deleted file on hard disc. “A lot of people think they are anonymous on the internet, but they’re not,” White said. “Every time they go to a porn site, for example, their IP address will be recorded. They’re just one subpoena away from being caught.”

A similar rule can be applied to managers and executives, he said. “There are a lot of people out there just waiting to be caught with documents they never thought would be produced against them.”

lgettler@theage.com.au