

| Electronic Data Retention Paper

October 2007

October 2007

Electronic Data Retention Paper

Contact



Cameron Abbott

Partner

T: +61 3 9640 4261

F: +61 9 9205 2055

E: cameron.abbott@middletons.com

Contents

Executive Summary	1
1.1 Document retention – legislation and case law	1
1.2 Electronic/imaged documents	2
1.3 Document security	2
1.4 Litigation	3
2. Legal Considerations for Document Control Policies	3
2.1 Why Have a Document Control Policy?	3
2.2 What do Document Control Policies Include?	4
2.3 Developing Policies for Document Retention	4
3. Specific Retention Obligations	5
3.1 Circumstances Where You Must Retain or Can Destroy	5
3.2 Consequences for breach?	6
3.3 Additional Legislative Retention Requirements	6
4. Common Law Requirements	8
4.1 The McCabe Case	8
4.2 Post McCabe – Legislation in Victoria	9
5. Legislation Regarding Digital Documents	10
6. Evidentiary and Record Keeping Issues	10
6.1 Best Evidence Rule	10
6.2 General Rules	11
6.3 What Evidence is Required?	11
6.4 Digitisation and Destruction?	12
6.5 Electronic Management of Public Records - Victorian example	13
7. Security Issues in an Electronic Environment	13
8. Corporate Governance	14
9. Developing Policies for Data Retention	15

Executive Summary

This paper summarises the following matters related to ensuring the legality, integrity and accessibility of electronic documentation:

- fundamental legal considerations for document control policies;
- specific retention requirements;
- legislation regarding digital documents;
- common law regarding digital documents;
- evidentiary and record keeping issues;
- the validity of email as an electronic document;
- security issues in an electronic environment;
- corporate governance requirements and potential liabilities; and
- developing policies for data retention.

Given the legal requirements relating to document retention in respect of financial and business records it is becoming increasingly important that organisations develop policies to support their legal obligations in relation to data retention. Add to this the increasing tendency of companies to conduct transactions and general business via email and over the internet, the importance of an effective electronic data retention regime and archiving system cannot be underestimated.

Effective document control policies will add to a business' effectiveness and therefore add to a strong reputation in the market. Such a policy should contain the following:

- the time period for which documents or files must be held;
- the reasons for decisions to retain or destroy the documents;
- the documents to which the policy will apply; and
- who is responsible for ensuring that procedures are followed

1.1 Document retention – legislation and case law

As a general note, specific document retention requirements are set out in several key pieces of legislation at both Commonwealth and State level in Australia. Various cases have supplemented the standards required in relation to document retention, such as the famous McCabe case regarding document destruction.

There are further obligations in other jurisdictions which apply to companies involved in e-commerce.

There are large penalties which apply for breaching legislative provisions which govern document retention, including criminal prosecution for breaches of the Crimes Act 1958 (Vic). Prosecution under the Crimes Act can attract penalties of up to 5 years imprisonment and \$330,000 fines. Further, breaches of the financial record retention requirements under the Corporations Act 2001 (Cth) (**Corporations Act**) can also attract fines of up to \$1,000,000 for corporations and \$200,000 for any individual involved in the breach – which means that directors need to be particularly careful to comply with the retention requirements from a personal perspective.

Further to the requirement to keep records under the various legislative regimes mentioned above, companies should be aware of the need to treat imaged documents in the same way as hardcopy documents, for the purposes of document retention and developing their retention policies. In Victoria (at least), the Limitation of Actions Act (Vic) 1958 establishes that in most cases corporations should keep electronic records for at least six years to bring proceedings in relation to breach of an electronic contract or defend against possible claims.

1.2 Electronic/imaged documents

Communications originating and being accessed electronically should be managed by an adequate and accessible system to identify the destination, time of sending and time of receipt of all such communications. This will ensure that such documents can be relied upon as evidence in accordance with the Electronic Transactions Act 1999 (Cth) (**ETA**).

In certain circumstances, the recording and retention of documents electronically may fulfil the legislative document retention requirements in place of the retention of hardcopy originals. However, businesses must ensure that their electronic records system complies with the requirements set out in the ETA to ensure the integrity of the record is maintained.

In order to ensure the appropriate information is retained, businesses are increasingly moving towards retaining emails and electronic documentation as part of their retention policy, to ensure that the documents are maintained and accessible in a way that will enable them to be relied upon as evidence in accordance with the ETA.

1.3 Document security

The potential for electronic security breaches has been well documented, especially in the current e-commerce environment. It is important to remember that security breaches can occur from both outside and within an organisation – a comprehensive document security policy should cover both occurrences.

Where the organisation stores personal information about its customers, the policy must ensure it complies with the requirements of the Privacy Act 1988 (Cth) (**Privacy Act**) to ensure adequate security safeguards are in place.

1.4 Litigation

The ultimate responsibility for creating and implementing electronic document control policies rests with a company's board of directors. Cases like McCabe illustrate that management must be aware that all recoverable electronic data is discoverable at law. All data is therefore valuable, and if unreasonably destroyed or missing, there are potentially severe consequences under the law.

Destruction of adverse documents may lead to:

- a charge of obstruction of justice.
- an adverse inference in litigation for failure to produce a document in litigation on the grounds that it was 'inadvertently' destroyed;
- the vicarious liability of the company for its employees' acts; and
- the personal liability of directors and officers for failure to implement appropriate corporate governance policies.

It is recommended that organisations obtain legal advice when developing their document control policy so as to ensure that it covers all the various legislative requirements.

From the above, it is clear that in an ever increasing e-commerce environment, organisations need to ensure they maintain and update appropriate electronic data retention policies to ensure that the organisation's management and board, together with the organisation itself, is not unduly exposed to harsh penalties under a range of applicable legislation.

2. Legal Considerations for Document Control Policies

2.1 Why Have a Document Control Policy?

There are innumerable legal and practical considerations relevant to the decision by a company to formulate a document control policy.

An effective document retention policy will achieve a balance between the requirement to retain and retrieve certain documents and the space and efficiency created when certain documents are destroyed. Given some of the software available today it is often easier to strike this balance with electronic data retention, given that it can be easier and more efficient to retrieve documents and eliminates the space constraints paper offices may have.

The proper handling of electronic documents has a significant impact on a business' performance and their professional reputation in the marketplace. As well as discharging corporate governance and legislative requirements, a structured approach to document retention is essential in promoting substantial business benefits as well as ensuring protection from the more obvious hazards, such as security and litigation.

2.2 What do Document Control Policies Include?

Policies are put in place to cover issues such as retention and destruction of documents whether electronic or paper. The aim of such policies is to completely monitor the life cycle of documents from creation to destruction. Typically a policy will determine:

- the time period for which documents or files must be held;
- the reasons for decisions to retain or destroy the documents;
- the documents to which the policy will apply; and
- who is responsible for ensuring that procedures are followed.

The myriad legal, technical and business issues converging on digital documents have the capacity to overwhelm, so it is essential that all employees and management of a company are aware of where respective responsibilities for compliance lie and any policy should clearly communicate this.

2.3 Developing Policies for Document Retention

To ensure a policy deals adequately with the types of documents and data used by an organisation, the organisation should:

- Analyse and categorise what data is required for business continuity;
- Determine if retention is required:
 - for current use;
 - by contract;
 - by law or regulation (general and industry specific legislation);
 - for business reasons;
 - for litigation or other special circumstance; or
 - for any combination of the above factors; and
 - If the relevant limitation period for retention is applicable.

Only if the answer is NO to all these questions may a document be destroyed... which means organisations and employees/management may be required to:

- retain a large number of documents;
- know their legal obligations regarding required time and form of data retention;
- accommodate Corporations Act, Income Tax Assessment Act 1936 (Cth) and Income Tax Assessment Act 1997 (Cth) (**Tax Acts**) and litigation considerations;

- implement consistent and effective policies and educate staff;
- in using electronic record management systems, put in place procedures to ensure the authenticity and integrity of the process; and
- ensure backup of information that will allow your company to operate and comply with corporate governance requirements.

3. Specific Retention Obligations

3.1 Circumstances Where You Must Retain or Can Destroy

Certain statutes will require that particular types of documents be retained for a certain period following their creation. This may include, for example:

- obligations under the Corporations Act to retain financial records:
 - s 1306: details the statutory requirements for maintaining business records in computer form. The company must take all reasonable precautions for guarding against damage to, or destruction or falsification of or in, any book or part of a book required to be kept or prepared by the company.
 - s 286: company must keep financial records that correctly record and explain its transactions and financial performance, and which would enable true and fair financial statements to be prepared and audited for 7 years.
 - 'financial records' includes invoices, receipts and documents of prime entry.
 - s 288: allows electronic storage provided records are available and can be converted into hard copy within a reasonable time.
- obligations under the Tax Acts and other tax legislation to retain supporting documentation:
 - s 262A(1)-(2): requires an entity to keep records that record and explain all transactions and other acts engaged in by the person that are relevant for the purposes of the relevant Act, that are in English or are readily convertible into English and that enable the entity's liability under the relevant Act to be readily ascertained.
 - s.262A(4): generally records must be kept for 5 years.
- obligations under Part VA of the Trade Practices Act 1974 (Cth):
 - manufacturers should keep records of products manufactured and/or sold for 11 years in case a situation arises where a consumer suffers injury, loss or damage from a product defect.

Certain industry codes of conduct and industry specific legislation which applies to an organisation may require retention of particular records, for example, the Health Records Act 2001 (Vic) and Financial Transaction Reports Act 1988 (Cth).

3.2 Consequences for breach?

Breaches of the financial records requirements of the Corporations Act can attract severe penalties. Failing to take reasonable steps to comply with, or secure compliance with, the Corporations Act can attract fines of up to \$1,000,000 for the corporation itself and up to \$200,000 for an individual that has failed to take reasonable steps to ensure compliance of the relevant provisions by the organisation. If such a breach is dishonest, the individual involved faces up to 5 years imprisonment or a \$220,000 fine. Another (or alternative) consequence for non-compliance may be disqualification from managing a corporation for a designated period.

Whilst breaches of other legislative requirements may not be as severe, it is worth noting the potential exposure to both the company and the individuals associated with the company, if the requisite records are not appropriately retained, as required by statute.

3.3 Additional Legislative Retention Requirements

3.3.1 Retention for Government Agencies- Victorian Example

The Public Records Office Victoria is responsible for establishing binding standards for managing public records. The Keeper of the Public Records (**Keeper**) is responsible for, amongst other things, the preservation and security of public records under his control and in this regard, issues standards for the classification and retention of such documents.

The Keeper has released a General Disposal Schedule for Common Administrative Records which identifies the specific time periods for retention of records. A person who removes, sells, damages or destroys a public record without authority is guilty of an offence (Public Records Act 1973 (Vic), s19); however, destruction or disposal of public records by a public officer in accordance with standards issued by the Keeper is lawful.

For example, financially accountable records may not be destroyed until audit requirements have been satisfied. Public offices which fall within the definition of a Department contained in Regulations under the Audit Act 1994 are required to obtain the consent of the Auditor-General prior to the destruction of financially accountable records.

3.3.2 Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (**ALCT Act**) imposes significant compliance and regulatory obligations on the financial services industry including the banking, life insurance, managed funds and superannuation sectors as well as gambling services providers and bullion dealers. These provisions relate not only to existing money laundering offences such as dealing in the proceeds of crime, but also to tax evasion.

The ALCT Act imposes a raft of new reporting and record keeping obligations including:

- the establishment of compliance programs to mitigate money laundering and terrorism financing risks;
- reporting requirements to AUSTRAC; and
- identification of customers and retention of records to verify such customers.

3.3.3 The Patriot Act (US)

Larger financial institutions which conduct much of their business electronically—and therefore are part of the e-commerce business sector—are affected by the Patriot Act (US) (**Patriot Act**). Among the provisions affecting large multinational financial corporations are:

- increased authority for US law enforcement officials to gain access to institutions' records and databases;
- due diligence by US financial institutions concerning money laundering by non-US persons;
- enhanced standards for correspondent accounts held by US banks; and
- prohibition of correspondent accounts with shell banks (banks which have no physical presence in their chartering country).

US financial institutions and organisations transacting with such institutions are required to consider and address how they will balance increased security provisions, broader access to their accounts by law enforcement officials, the retention of certain records and ensuring customers that the privacy and integrity of financial accounts will not be compromised by compliance with the Patriot Act.

3.3.4 Sarbanes –Oxley Act (US)

The Sarbanes-Oxley Act was enacted in 2002, and introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws".

Organisations with US operations or links should be aware of specific requirements which relate to:

- periodic statutory financial reporting;
- publication of accurate financial statements;
- document retention requirements which evidence adequate internal controls and procedures; and
- disclosure of material changes in financial conditions or operations.

4. Common Law Requirements

In addition to the statutory obligations discussed above, the common law imposes obligations to retain records, which are or may become relevant to litigation:

- it is clear that once litigation is commenced, there is an obligation upon all participants to retain all records relevant to the litigation; and
- prior to the actual commencement of litigation, where the anticipation of litigation is present, all records potentially relevant to that litigation may need to be retained, even before notice of commencement of proceedings.

4.1 The McCabe Case

Recent common law has addressed the question of what degree of knowledge of actual or impending litigation a person must have before they can lawfully destroy documents potentially relevant to a claim or defence. Once proceedings begin, a corporation is obliged to preserve all potentially relevant documents.

The case of British American Tobacco (BAT) v McCabe¹ (**McCabe Case**) is instructive in relation to the provision of e-documents during discovery. This decision showed that even when a company has a "document retention policy" in place to facilitate provision of e-documents in the event of discovery orders, this may not guarantee the company's policy will be spared exhausting judicial scrutiny. On appeal² the issues of intention and anticipation were crucial.

The Victorian Supreme Court of Appeal held that no company's so called "retention policy" can be seen to possess a positive intention to destroy materials for the purpose of preventing their disclosure at future or imminent litigation. Further, where a company is not actually on notice of impending litigation but litigation could be 'anticipated' by a company, it remains undecided whether a company can or should continue normal wholesale document destruction, particularly if the type of documents destroyed could be later shown to have been relevant to a later case.

In 2004, the Queensland Supreme Court upheld a Queensland District Court decision which convicted a person for attempting to pervert the course of justice where that person had shredded papers knowing they 'might' be required in judicial proceedings (R v Ensbeys [2004] QCA 335). This decision is of particular significance because until this time, every State jurisdiction had maintained that there must be legal proceedings under way at the time records are destroyed before such a charge could be laid against an offender.

It has been contended that in light of this judicial shift, a new standard of 'anticipation' of litigation has been established in Australia. The issue of foreknowledge remains in the balance. However, the decision in Ensbeys and the statement of the Court in McCabe seem to demonstrate a judicial shift towards a higher standard of anticipation of proceedings. A sound document retention policy will be necessary more than ever before in light of these decisions.

¹ [2002] VSC 73 (22 March 2002).

² [2002] VSCA 197 (6 December 2002).

4.2 Post McCabe – Legislation in Victoria

The Crimes (Document Destruction) Act 2006 (Vic) (**Crimes Document Destruction Act**) amends the Crimes Act and creates a new criminal offence in relation to the destruction of documents likely to be required in legal proceedings. An employee or officer performing the relevant act of destruction who knows of the reasonable likelihood of litigation and intends to prevent the document from being used, could be prosecuted for document destruction. Both individuals and companies can be prosecuted, potentially facing large fines and imprisonment.

A company may be vicariously liable for an officer who breaches the document destruction provisions of the Crimes Act; however, the liability of the company does not hinge on the officer being prosecuted.

A company may argue that it exercised 'due diligence' to prevent the breach and bears the onus of proving this. In this regard, the 'corporate culture' of a company would be examined as to whether appropriate document retention protocols and risk management strategies are in place to illustrate the 'due diligence' requirement. In light of the growing use, reliability and accessibility of electronic document retention alternatives, companies must appreciate the increasing difficulties and perils associated with justifying document destruction and the failure to implement appropriate policies.

The Legislative Council passed this Bill on 28 March 2006 and it received Royal Assent on 4 April 2006. Subsequently, the Crimes Document Destruction Act came into effect on 1 September 2006.

Criminal prosecution applies for breaches of these new provisions, with penalties of up to 5 years imprisonment or fines of up to \$330,000.

5. Legislation Regarding Digital Documents

When formulating document retention policies, companies should note that subject to specific requirements, an imaged document is admissible as evidence and will effectively be treated as an original document under the Commonwealth Act.

Pursuant to section 48 of the Evidence Act 1995 (Cth) (**Evidence Act**), a party may adduce evidence of the contents of a document in question by tendering the document in question or by tendering a document that:

- is or purports to be a copy of the document in question; and
- has been produced, or purports to have been produced, by a device that reproduces the contents of the document.

Section 146 of the Evidence Act 1995 (Cth) creates a rebuttable presumption in favour of the person adducing evidence that is produced by a particular device or process that:

- the particular device or process was operating correctly at the time the document was produced; and
- the device or process ordinarily produces a particular outcome (an imaged document that was an exact copy of the original for instance).

However, it is open to a party to adduce evidence that rebuts this presumption.

Any limitation of actions legislation should also be kept in mind in formulating an effective electronic document retention policy. In Victoria, the Limitation of Actions Act (Vic) 1958 establishes that in most cases corporations should keep electronic records for at least six years to bring proceedings in relation to breach of an electronic contract or defend against possible claims.

6. Evidentiary and Record Keeping Issues

6.1 Best Evidence Rule

A starting point in considering the laws of evidence applicable to proper record keeping is the "best evidence rule". The rule requires litigants to present the "best evidence" to the court, rather than a copy or some secondary record of the same evidence. Specifically, it requires the production of the original of any document by the tendering party to prove its contents, unless the absence of the original can be explained. For example:

- the original has been lost;
- it is impractical or unduly burdensome to produce the original, or
- the original is a public record in the custody of the state archives and a certified copy is available.

Even without amendment to the best evidence rule, if an original document had been destroyed as part of a legitimate digital recording process, it is likely that the destruction would be explicable and the digital record would have become the "best evidence" required for production to the court. In such circumstances, the rule may not require the original documents to be saved in case of litigation.

6.2 General Rules

The ETA deals with the validity of electronic transactions in commercial transactions. Section 8 provides that for the purposes of a law of the Commonwealth, a transaction is not invalid because it took place by means of electronic communication. The ETA facilitates electronic commerce by removing existing legal impediments that formerly prevented people using electronic communications to satisfy legal obligations under statutory law. The ETA identifies four types of requirements under a law of the Commonwealth that can be met in electronic form:

- a requirement to give information in writing (section 9);
- a requirement to provide a signature (section 10);
- a requirement to produce a document (section 11); and
- a requirement to record or retain information (section 12).

6.3 What Evidence is Required?

In general, digital documents will only be considered to be valid and admissible as evidence in litigation if they can be authenticated. In assessing the authenticity and integrity of such documents, a number of factors are often considered, including:

- are electronic signatures used to identify the originator of the digital record?
- are formalized business processes and procedures in place to verify the production of digital records in the course of business?
- are formalized business processes and procedures in place to verify the secure storage of digital records?
- can audit trails easily be produced to trace the movement of the digital record in the organisation?

In the case of electronic communications, it is critical that there is an adequate and accessible system in place to identify the destination, time of sending, and time of receipt of all such communications.

6.4 Digitisation and Destruction?

Section 12 of the ETA, relating to the recording and retaining of information electronically, is particularly relevant to organisations wishing to scan paper based records and retain the electronic copy instead of the paper. The ETA does give justification for a business decision to scan paper records and retain the scan as the record, yet there are some limitations on its effectiveness in mitigating potential concerns about electronic records:

- Process matters: The scan must be produced through a process capable of ensuring and maintaining the integrity of the record over time. Scanned copies are only as good as the process that produced them, which should include authentication and quality assurance, for example:
 - name, address and occupation of individual doing the scanning;
 - identity or description of the documents, a description of the file, where they came from and their condition;
 - identify object/ medium upon which the document is being stored;
 - the day of scanning; and
 - endorsement (or noting, by tick in a column or the like) that scanning machine in good working order, scanning done in ordinary course of business and signature by person scanning that above information is true and correct.
- Format matters: Must be in a format and environment that makes it readily available for subsequent reference. Selecting appropriate technology that will allow access to documents down the track seems to be the greatest challenge for organisations. Many have chosen to store documents in PDF format, which has become an almost de facto standard.³ However, where people choose to store documents in their native format, for example in programs like Excel or PowerPoint, they face greater risk that in 10 years time they may not be able to open these files.⁴ The Victorian Electronic Records Strategy (VERS), developed by the Public Record Office of Victoria, supports the use of CD-ROMs for document storage.⁵ It is important, however, to choose long life CD-ROMs.
- Timing matters: As the ETA has yet to be considered by a court in any detail, it is not certain how the courts will treat scanned copies where paper originals have been destroyed. While it is likely that the implementation of a standard, approved digitisation process will render the scans admissible, there is a risk in adopting this strategy in advance of any legal decisions.
- Technical process involved: It is also important that technical processes are adopted to ensure that information remains complete, unaltered and unaffected by any material changes over the course of storage.⁶ Where this cannot be guaranteed, courts are likely to require at least that there be an audit trail of any changes made.⁷

³ Phil Farrelly in Kellie Harpley, 'Files in transition', *Lawyers Weekly*, 14 April 2006, 19.

⁴ Ibid.

⁵ Ibid.

⁶ Kellie Harpley, 'Files in transition', *Lawyers Weekly*, 14 April 2006, 19.

⁷ Ibid.

6.5 Electronic Management of Public Records - Victorian example

The Keeper of Public Records has released guidelines for government agencies regarding the processing of public records in electronic form. The Standard for the Management of Electronic Records (PROVS 99/007) mandates conditions and requirements for the management and preservation of electronic records in the Victorian public sector.

These guidelines are instructive to any organisation developing procedures for effective and lawful electronic records management.

Briefly, an electronic records format used by a government agency must be able to support:

- Long life. Records must have an indefinite life. That is, the contents of a record must be capable of being viewed forever. This has three aspects:
 - Preservation. The records must be in a form that can be physically preserved (for example easily copied from one media to another without loss of quality).
 - Accessibility. It is useless to save records unless they can be found again.
 - Readability. Records must be able to be viewed as the creators and users originally saw them.
 - Comprehensibility. Records must be able to be understood in their context.
- Evidence. Electronic records must be admissible as evidence and given due weight in a court of law. This requires the ability to prove that a record has not been altered in an unauthorised or undocumented fashion since creation, and to demonstrate who created the record and when it was created.
- Disposal. It must be possible to dispose of records (that is, evaluate and determine the record's status) and, where authorised, subsequently transfer or destroy records in a controlled manner.
- Modification. It must be possible to be able to modify a record without disturbing the evidentiary integrity of the record.

7. Security Issues in an Electronic Environment

Document security is an imperative aspect of any document retention policy, but is of particular importance in the electronic environment.

The potential for electronic security breaches has been well documented. It is important to remember that security breaches can occur from both outside and within an organisation – a comprehensive document security policy should cover both occurrences.

The potential consequences for businesses include:

- direct financial loss and exposure to breach of contract actions from clients for failing to keep their information secure;

- exposure to liability for subsequent client loss;
- damage to reputation;
- an inability to comply with legal requirements for operating a company; and
- loss of corporate governance data.

Relevant legislation includes:

Privacy Act

Organisations that store personal information must ensure the integrity and security of such information and are susceptible to:

- investigation by the Privacy Commissioner in the event of a complaint.
- Information Privacy Principle 4 requires that the record keeper must ensure
 - that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
 - what is "reasonable" will depend on the circumstances in which the personal information is held – higher levels of security will be expected for more sensitive information.

Corporations Act

- Directors may be in breach of their duty to their company if they fail to adequately protect the company from security violations.

8. Corporate Governance

Companies need to be in a position to confront the realities of litigation, as commercial cases comprise the bulk of all litigation before the courts. To this end, a solid document control policy is required.

The ultimate responsibility for creating and implementing electronic document control policies rests with a company's board of directors. Cases like McCabe illustrate that management must be aware that all recoverable electronic data is discoverable at law. All data is therefore valuable, and if unreasonably destroyed or missing, there are potentially severe consequences under the law.

The destruction of adverse documents is most serious and may lead to the following consequences:

- a charge of obstruction of justice. Legislation in various jurisdictions makes it an offence to destroy any document that is or may be used as evidence in a judicial proceeding (as discussed above); or

- failure to produce a document in litigation on the grounds that it was 'inadvertently' destroyed may lead to an adverse inference in litigation.

Additionally, companies must also consider:

- the possibility of vicarious liability - companies are responsible for the acts of an officer and employee within the scope of his or her duties; and
- directors or officers (potentially CIO) can be personally liable for failure to implement appropriate corporate governance policies.

9. Developing Policies for Data Retention

Ultimately, companies should ask:

"Have we contemplated the realities of:

- (a) specific retention requirements;
 - key legislation (Corporations Act, Sarbanes-Oxley, Anti-Money Laundering etc); and
 - common law (McCabe, Ensbey);
- (b) evidentiary and record-keeping issues;
- (c) security issues in an electronic environment; and
- (d) corporate governance requirements and potential liabilities, and the demands each would place on the company and its electronic document assets?"

It is essential that businesses create and implement appropriate document retention protocols in order to manage the risks and potential rewards of handling electronic documents efficiently and safely.

We note that shortly before the time of publication it has been foreshadowed that the Federal Court of Australia will soon be implementing a new set of rules on discovery (in litigious proceedings) in respect of electronic documents. These rules will be incorporated into the relevant guidelines for the Supreme Court of Victoria. Now, more than ever, businesses will need to ensure electronic documents are appropriately stored and retained.

