

# BE CAREFUL WHAT YOU **shred**

Susan Bennett, a partner with Sparke Helmore Lawyers, discusses the importance of directors ensuring that their companies have comprehensive information management policies in light of recent Victorian legislation.

FROM 1 SEPTEMBER 2006, the destruction of a document that is likely to be required in evidence is a criminal offence in Victoria. While this new law results from the amendment to the Victorian *Crimes Act 1958*, it is having a significant impact upon the way companies throughout Australia manage the retention and destruction of documents and information.

The document destruction legislation in Victoria imposes serious penalties on individuals and companies involved in the destruction of documents. Together with existing obligations, including those under the *Corporations Act (2001)* it provides a timely reminder for directors and senior management of the need to review and assess the adequacy of information management policies in their company.

Directors need to satisfy themselves that appropriate mechanisms are in place to ensure that the information management policy complies with all legal and regulatory requirements and that this policy is properly implemented throughout the organisation.

#### Background to the new legislation

The *Crimes (Document Destruction) Act (Vic)* and the *Evidence (Document Unavailability) Act (Vic)* came into effect on 1 September 2006. Together these acts form part of the Victorian Government's package of legislative measures to address the legal and policy implications arising from the Victorian Court of Appeal decision in 2002 in *British American Tobacco Australia Services Ltd v Cowell* (also known as the McCabe decision).

After the McCabe decision, the Victorian Attorney-General commissioned the Crown Counsel of Victoria, Professor Peter Sallmann, to make recommendations about the key public policy considerations arising from the case. The introduction of both Acts flows from the recommendation by Professor Sallmann that Victoria should introduce a criminal law provision to deal with instances of document destruction relevant to legal proceedings.

While it is already an offence to destroy evidence relevant to a current judicial proceeding in most jurisdictions in Australia (under the various state Crimes Act or Criminal Codes), the *Crimes (Document Destruction) Act (Vic)* imposes more stringent obligations for proceedings in Victoria and consequently for any company that may be involved in legal proceedings in Victoria.

Under the *Document Destruction Act* it is a criminal offence to destroy documents that are, or are reasonably likely to be, required in evidence in legal proceedings in Victoria. Given the definition of 'legal proceeding', the offence will extend not only to court proceedings, but to any proceeding or inquiry before any person acting judicially (including, for instance, arbitrations and administrative or public hearings).

The penalties include:

- up to five years imprisonment; and/or
- a fine of up to \$64,458 for an individual or \$322,290 for a company.

#### Liability of employees and companies

Under the *Document Destruction Act* a person will be guilty of an offence if they know that a document (or any other thing) is, or is reasonably likely to be, required in evidence in a legal proceeding (whether the proceeding has been commenced or may be commenced in the future) and they:

- destroy or conceal it; or
- 'expressly, tacitly or impliedly' authorise another person to destroy or conceal it with the intention of preventing it from being used as evidence.

If a director or officer of a company commits the offence, not only will the individual be liable, but the offence can also be attributed to the company itself. Where an employee commits the offence, the company can still be held liable in the event of a finding that 'a corporate culture existed within the company that directed, encouraged, tolerated or led to the offence being carried out'.

'Corporate culture' is defined in the *Crimes (Document Destruction) Act 2006* as an "attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant conduct is carried out or the relevant intention formed."

The issue will be whether the corporate culture encouraged or allowed document destruction to be carried out and this will depend on the facts and circumstances of each case.

---

*Directors need to satisfy themselves that appropriate mechanisms are in place to ensure that the information management policy complies with all legal and regulatory requirements and that this policy is properly implemented throughout the organisation.*

---

#### Defences - due diligence

Section 255(3) of the *Document Destruction Act* provides that it is a defence for the company to prove that it exercised due diligence to prevent the contravention by the officer or employee. It will be interesting to see how courts assess whether a company 'exercised due diligence'. However, factors that are likely to be taken into account include whether or not:

- there is a current information management policy that complies with all legal and legislative obligations;

- the information policy balances in good faith both the retention and destruction of information;
- all employees are aware of and act in accordance with the policy; and
- in practice the policy is applied throughout the organisation.

#### Document Unavailability Act

Under the *Document Unavailability Act* where a document has been destroyed or is unavailable, and its unavailability is likely to cause unfairness to a party to the proceeding, a court may order that:

- adverse inferences be drawn from the unavailability of the document;
- a fact in dispute be presumed in the absence of evidence to the contrary;
- certain evidence not be adduced;
- all or part of a defence or statement of claim be struck out; or
- the evidential burden reversed in relation to the fact in issue.

#### Courts' powers

These proposed rulings or orders follow the type of orders that have been made in high profile US cases involving destruction of documents. In some cases, juries have awarded substantial damages as a result of judges making directions against the party who has destroyed or made unavailable documents that are now available to judges under the *Document Unavailability Act*.

In the case of *Zubulake v UBS Warburg*, the jury awarded a former UBS equities trader \$US29.3 million in damages for what was described by the judge as a "relatively routine employment discrimination dispute in which discovery lasted over two years."

One of the orders made by the court was that the jury empanelled to hear the case be given an adverse inference instruction with respect to the emails deleted after the litigation hold order. The basis for the direction was the failure to preserve back-up tapes and the fact that UBS had in contravention of the 'litigation hold' instructions deleted relevant emails that were later recovered from alternate sources, and then provided to the plaintiff some two years after the document requests.

In *US Government v Philip Morris USA*, Philip Morris were ordered to pay \$US2.75 million to the court as punishment for failing to comply with a court ordered preservation order. Employees of the defendants who received notice of this preservation order continued to delete emails for at least two years after the preservation order was issued, in some instances in contravention of Philip Morris' own internal document retention policy.

In addition to the fine, the court precluded Philip Morris from calling as witness or experts anyone who had failed to comply with Philip Morris' own internal document retention policy. This meant that Philip Morris was unable to call a number of their key witnesses.

#### Practical implications

The following questions need to be asked and considered by directors when reviewing a company's information management policies:

- does it comply with all relevant legislative and regulatory obligations?
- does it comply with Australian standards and best practice?
- is the policy implemented throughout the organisation, including:
  - are employees (particularly new employees) provided with training?
  - is there a comprehensive process for archiving both hard copy and electronic documents - including email?
- are information management policies regularly reviewed and updated to ensure compliance with legislative and best practice developments?
- does it include appropriate 'legal hold' mechanisms to ensure that documents required for actual or anticipated litigation are preserved and are able to be identified and collated in an efficient manner? **Ⓛ**

## BoardHub

when you need the best

board & committee  
document distribution

- ✓ full functionality
- ✓ real security
- ✓ true ease-of-use

[www.boardhub.com](http://www.boardhub.com)



CommandHub Pty Ltd  
Level 27, 101 Collins Street,  
Melbourne Victoria 3000  
03 9653 9585