Information Management Advice 16 Legal Acceptance of Records

Introduction

The changes to evidence law contained in the Evidence Act 2001 mark a significant turning point in the admissibility of evidence presented before Tasmanian courts. This legislation contained significant changes to rules of evidence making it much easier for records created in electronic systems to be admitted in evidence.

The Evidence Act relaxes and, in some cases, removes restrictions on evidence which can be admitted in proceedings (particularly civil proceedings), so that a greater range of relevant evidence is available to courts for fact finding purposes. The Act contains major reforms to the laws of evidence, in both civil and criminal proceedings, and the manner in which evidence is given.

In relation to documentary evidence, the reforms made by the Act include:

- ***a narrower hearsay rule and wider exceptions to that rule, providing for greater admissibility of hearsay evidence;***
- ***abolition of the original document rule, replacing it with simple means of giving evidence of the contents of documents, including documents held in computer and other non-paper forms;***
- ***provisions for easier proof of, and presumptions about, business and official records, and the use of mail, fax and other means of communication; and***
- ***pre-trial procedures enabling litigants to test the weight of documentary evidence that might be given in proceedings.***

With a greater range of evidence being admissible in many Federal and Tasmanian courts, an important consideration in most cases will be the quality of evidence that might be available in a proceeding and whether it is likely to persuade a court to accept that the Crown's version of the facts is correct.

It is essential for agency managers to ensure their accountability practices and recordkeeping systems can stand up to the scrutiny of the courts as well as Parliament, the Ombudsman and relevant auditors. Important stakeholders in this process are individual citizens who have rights of redress through the institutions mentioned and who also have access to records and other information through the Right to Information Act 2009 and the Archives Act 1983.

This advice is provided to assist agencies assess the legal implications of current Tasmanian and Commonwealth Evidence Acts, to ensure the legal acceptance of their records, particularly electronic records.

The legal environment

Evidence introduced into legal proceedings in Tasmania is subject to a range of Tasmanian and Commonwealth legislation and to the common law. Where it is necessary to use agency records in court proceedings, different laws of evidence apply depending on the court in which the proceeding is being heard and the type of document that is to be used.

If the proceeding is in a Tasmanian court, the evidence law which applies is set out in the *Tasmanian Evidence Act 2001*. If the proceeding is in a Federal court, the *Commonwealth Evidence Act 1995* applies. The *Tasmanian Evidence Act* is mirror legislation to the *Commonwealth Evidence Act* and consequently has the same admissibility requirements.

In addition, some provisions of the *Commonwealth Evidence Act* also apply in Tasmanian court proceedings in relation to some documents (eg a document signed or sealed in an official capacity, a government gazette or other officially printed document, a document published by the Australian Statistician, and a 'public document' or a 'Commonwealth record' within the meaning of the *Evidence Act*). As well, specific State laws, and state records guidelines may apply to particular records. For example the *Archives Act 1983, Right to Information Act 2009*, and *Personal Information Protection Act 2004*.

The rules of evidence

The rules of evidence govern how a party goes about proving its case in a legal proceeding.

The courts must determine the facts of each case. The focus of the rules of evidence is to assist the Court in the establishment of the facts.

Parties seek to persuade the court by producing evidence. A party, which wants to persuade a court of a fact, such as a fact asserted in a document, must address three questions:

- how to adduce (that is, put to the court) evidence of the fact;
- whether the court will permit the evidence to be given (that is, whether it is admissible);
- the weight of the evidence (that is, how much importance the court will give to it in reaching its decision).

The rules of evidence are mainly concerned with the first two issues. They specify:

- how information, in the form of 'evidence', is given or presented to a court;
- whether that information can be given or led in a proceeding.

If particular evidence cannot be given or led in a proceeding, the evidence is said to be 'inadmissible'.

The new rules of evidence make it easier to adduce evidence and to remove restrictions on inadmissibility, especially in relation to documents. However, this does not affect the need to ensure that the evidence available is of high quality. Assessment of the quality of evidence (of the weight to be given to it) is a matter for the court in each case.

The distinction between admissibility and weight of evidence

Although evidence of information about a particular fact is admissible in a proceeding, it does not mean that the court will necessarily believe or act on that evidence. If the information about the fact is a witness's direct observation, the court may simply disbelieve the witness for a variety of reasons.

More usually, evidence of information given in court will not be 'direct observation' evidence. Instead it will be evidence that suggests, or from which it can be inferred, that a particular fact occurred.

For example...

The Crown needs to prove the time that John, a public servant, arrived at work on a particular day. There may be no 'direct observation' evidence of that fact, that is, nobody who saw John arrive at work on the day in question, noted the time, and can remember it. Yet there may be other evidence that suggests that John arrived at a particular time on that day. There may be evidence that:

- he logged on to his work computer using a personal password at a particular time on that day, or
- he entered a particular time in his electronic flexitime attendance sheet recording that time as the time of his arrival.

Even if the evidence is admissible and is admitted, whether or not the court will accept the evidence that John was at work at that time may depend upon other evidence before the court, including evidence that may be led by another party.

For example, the Crown's evidence of an electronic record of John's computer log-on time may need to be accompanied by evidence that John's password was one that was personal only to him and, in the case of a network computer system, that John could not 'log-on' from a place other than his place of work.

But that evidence may not mean that the court would necessarily infer that John was at work at that time if there were some other evidence before the court, for example, suggesting that personal passwords for people in John's work area were generally known and occasionally used by other people to log on to the work computer or that electronic attendance sheets were susceptible to alteration by other people since the time of John's original entry.

How evidence of information in a document can be given

The rules of evidence under the Tasmanian and Commonwealth Evidence Acts apply to a document that is a 'record of information'. The term 'document' is defined in the Interpretation Section of the *Evidence Act 2001* to mean:

> "…any record of information and includes -
> (a) anything on which there is writing; or
> (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or
> (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
> (d) any map, plan, drawing or photograph; …"

The rules apply to an ordinary document in writing, documents written in braille or shorthand and, importantly for modern record management systems, to a 'record of information' that is contained on a computer (or audio or video) tape or disk, or optical laser disks.

Tasmanian and Commonwealth Evidence Acts abolish (in courts where they apply) the common law 'original document rule', which requires the production of the original document in writing, and permit evidence of the contents of a document to be given in one of a number of alternate ways. These ways include tendering:

- the original document;
- a copy of the document produced by a device (such as a photocopier or a word processor) that reproduces the contents of documents;
- a transcript of a document recording words (such as an audio tape or shorthand notes);
- a printout of computer output or a document reproducing the contents of an optical laser disk; or
- a business record being an extract, summary or copy of the document

Other ways may be used to give evidence of official documents, and documents that are unavailable to a party in the proceedings, for example, where they have been lost or destroyed.

While the 'original document rule' has been abolished, it is still necessary for parties to authenticate evidence of the contents of documents given by one of these alternate ways. For example, in relation to a document in writing that is signed, it remains necessary to lead evidence (if the point is contested) that the signature appearing on the document is the signature of the person who has purported to sign it. In the case of computer records, it is necessary to give evidence that the computer output is what it purports to be.

While there are several provisions of the Act facilitating this authentication process, the Act also sets out procedures under which litigants may test the authenticity of evidence of the contents of documents that are or might be led under one of the alternate ways in a proceeding.

The procedures, which can be set in train before the hearing of a proceeding, may result in the making of court orders against the party leading evidence of the contents of the document, including an order that:

- the original document be produced;
- a party be permitted to examine, test or copy a document;
- a person concerned with a recordkeeping system be called to give evidence; or
- in the case of a computer or similar document, that a party be permitted to examine and test the way in which the document was produced or has been kept.

The ultimate sanction for failure to comply with such an order is that the evidence of the contents of the document is not to be admitted in the proceeding.

How evidence of information in a document may become inadmissible

A separate issue from how evidence of information in a document can be given is whether the court will permit the evidence to be given - that is, whether the evidence is admissible in the proceeding before the court.

Whether the evidence is admissible depends, initially, on whether it is relevant to a fact in issue in the proceeding. If relevant, evidence may nevertheless be inadmissible if it is excluded by a rule that excludes

evidence, such as the rule against hearsay evidence, the 'similar fact evidence' rule, and the rule against opinion evidence.

The most important exclusionary rule in relation to documents is the hearsay rule. The hearsay rule applies when evidence of what is contained in a document is being used to prove some fact asserted in it.

For example, to return to John's time sheet...

The hearsay rule will apply to the use of evidence of the entry made by him of the time of his arrival to prove he was at work at that time.

Unless an exception to the rule applies, evidence of the entry will be inadmissible to prove that John was at work at that time, as the entry may have been made at a time other than the recorded time.

The hearsay rule under the Tasmanian and Commonwealth Evidence Acts

The hearsay rule provides that evidence of a previous representation (oral, or written statement) made by a person is not admissible to prove the existence of a fact that the person intended to assert by the representation.

Under the Acts the rule applies to every statement made by a person in a document, if evidence of the statement is led to prove the existence of such an asserted fact. In relation to electronic records, the rule does not apply to machine produced information as such information is not a 'statement made by a person'.

When the hearsay rule applies, exceptions to the rule exist for:

- evidence admitted for a non-hearsay purpose (where the statement is relevant for a purpose other than to prove the existence of a fact that the person intended to assert by the statement, for example, where the fact that the statement was made is relevant). In such a case evidence of the statement can also be used as evidence of what is asserted by the statement;
- first-hand hearsay, the scope of the exceptions depending upon whether the proceeding is civil or criminal and whether the person who made the statement is available or not to give evidence;
- some categories of more remote hearsay (that is, where the evidence is not necessarily first-hand hearsay), such as some statements in business records, some tags and labels or writing attached to or placed on objects (including documents) in the course of a business transaction; and
- an admission made by a person who is or becomes a party to the proceeding.

Some procedural safeguards apply for some of these categories of hearsay evidence. For example, notice provisions where the person who made a statement admitted under one of the exceptions for first-hand hearsay is not to be called to give evidence in the proceeding, and other procedures under which a party may be required to call as a witness the person who made the statement.

Compliance with subpoenas and orders for discovery

Occasionally, agencies need to comply with requirements imposed by courts to produce or disclose documents needed for legal proceedings, including proceedings in which the Crown is not a party. These requirements usually arise following the issue and service of a subpoena or similar document in a proceeding, or by way of an obligation or court order to give discovery.

A subpoena is a court order requiring the giving of evidence, or the production to the court of documents, or both. Discovery is the process whereby parties to court proceedings identify and disclose to each other documents which are relevant to the issues in the proceedings. Discovery only relates to disclosure of documents, and not to the giving of evidence.

In some courts, an order for discovery may be made against a person or a body who is not a party to the proceedings. Substantial obligations may be imposed upon agencies to whom a subpoena, or an order for discovery, is directed. Both processes require the agency to whom an order is directed to make a full and thorough search for relevant documents, including documents held in an electronic form.

Depending upon the circumstances, failure to comply with relevant requirements (eg to produce to the court all documents falling within a stated description) may result in the agency being found in contempt of court.

Recordkeeping requirements

The *Electronic Transactions Act 2000* facilitates electronic communications and the *Evidence Act 2001* changes the requirements for admissibility of evidence for records created or maintained in electronic systems. These changes and the need to comply with subpoenas and discovery orders have significant implications for the management of agency records and the development and maintenance of recordkeeping systems, particularly where those recordkeeping systems are in electronic form. Efficient and prudent recordkeeping and information systems should, therefore, be designed so that records that may need to be produced or disclosed for legal proceedings, often within quite tight deadlines, can be readily identified and located.

Reviewing recordkeeping practices

As government agencies make increasing use of newer technologies for recordkeeping and information management, such as electronic document management, digital imaging, electronic messaging, workflow management, electronic commerce and other electronic information systems, recordkeeping practices should be reviewed so that agencies continue to produce and capture proper records which are authentic, reliable, and accurate for legal, audit, and other purposes. Section 10 of the *Archives Act 1983* requires all relevant authorities to make proper records of the business of their organisations and keep them until they are dealt with through other sections of the Act.

Agencies should take special precautions when using newer technologies to enhance the reliability of their recordkeeping systems to increase the likelihood that records produced by such systems will be legally acceptable. Establishing the authenticity and reliability of records may depend on the accuracy of the process or system used to produce the record, the source of the information in the record, and the method and time of its preparation. Problems may arise with admissibility if appropriate procedures are not followed in creating and maintaining records.

Establishing a recordkeeping and systems management regime

Meeting evidentiary requirements in a complex, changing technological environment is a challenging undertaking that requires cooperation and coordination within agencies. To ensure that proper records are created and maintained, an agency must maintain a comprehensive, credible information and recordkeeping regime. Such a regime requires formal organisational arrangements and clarification of responsibilities in relation to the management of records. These should be stated in policies and procedures relating to records management and recordkeeping systems. Agencies must ensure the appropriate numbers, quality, and proficiency of people responsible for stewardship of an agency's information assets, including records. With the growth of decentralised computing and distributed electronic information systems, each user must assume responsibility for producing and maintaining authentic, accurate and reliable records within organisational recordkeeping systems and be supported by rules, procedures and training to ensure an understanding of individual requirements.

In summary, corporate managers, records managers, information managers, web content managers, administrative support staff, and information technology professionals need to all be involved in the recordkeeping process to ensure that authentic, accurate and reliable records are produced and retained.

For the establishment of an appropriate recordkeeping regime agencies need to:

- undertake a strategic analysis of corporate information and recordkeeping requirements;
- produce written policies and procedures to define normal operations for development, maintenance, and use of electronic information and recordkeeping systems;
- provide training and support to help ensure that policies and procedures are understood and implemented by staff;
- ensure recordkeeping requirements are built into electronic information systems to enable the capture of appropriate records; and
- ensure that records in electronic recordkeeping systems are only disposed of in accordance with authorisation provided by the State Archivist.

In addition to undertaking steps to ensure appropriate recordkeeping regimes are established agencies also need to ensure that an appropriate systems management regime is in place to support the business of the organisation and the authenticity of records. Agencies need to:

- develop adequate system controls to ensure the quality and reliability of the records created and maintained by electronic systems;
- develop and implement system audit trails to detect who had access to the system, whether staff followed certain procedures, or whether fraud or unauthorised acts occurred or might be suspected in the system;
- conduct routine tests of system performance. Automated information systems rely on system edits and routine testing to verify the accuracy and validity of data. System edits define the parameters of on-line system processing. Tests of system performance, conducted on a routine basis, provide necessary oversight to verify the integrity of a system;
- routinely test and document the reliability of hardware and software using a plan developed with the advice of the manufacturer, retaining all documentation related to hardware and software procurement, installation, and maintenance, and maintaining

operation logs and running schedules to document the reliability of system operation and performance;
- provide adequate security by developing routines that limit access and update privileges to the appropriate people and prevent unauthorised modification of data;
- establish controls for accuracy and timeliness of input and output through systematic procedures for data entry;
- reach agreement on issues relating to data exchange including provisions for the structure and format of data into transactions sets, the standards for communication, and security procedures;
- create and maintain comprehensive system documentation on all aspects of system design, implementation, maintenance, and oversight; and
- retain documentation describing how a system operated and describing the purpose, structure and origins of data for at least as long as any records produced by a system are retained.

As well as conforming with *State Records Guideline No. 8, Digitisation and Disposal of Source Records* agencies using digital imaging technology should also implement the following measures as part of the normal operation of the imaging system:

- mechanisms for verifying that the system accurately reproduces originals based on recognised industry standards and procedures;
- use of standard compression and decompression algorithms;
- thorough description of any image enhancement techniques in the system's documentation;
- stringent security provisions to prevent alteration of digital images; and
- use of Write-Once-Read-Many (WORM) optical media for imaging applications.

Recommended Reading

Standards Australia, Guidelines for the management of IT evidence.[1]

[1] www.standards.org.au

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

Acknowledgement is made to the National Archives of Australia, *Commonwealth Recordkeeping – Overview – Records in Evidence* for much of the content in this advice, and to the Crown Law Office, Department of Justice, for advice and assistance with the legal aspects of this guideline.

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	February 2015	Christine Woods	Template	All
1.0	14-12-2005	AOT	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template

Issued: December 2005

State Archivist