Revision

- What is information policy?
- The socio-legal context
- The weight of the law

The big picture

[Diagram showing relationships between recorded information, information product, information by-product of business activity, compliance, juridical systems/socio-legal context, communication technologies, statutes/laws, codes/standards, ethics.]
The difference that records make

- Information products and by-products raise different legal issues and are subject to different laws in most cases
- For example, Copyright, Defamation and Contract Laws versus Privacy and Evidence Laws

Specific legislation 2: Evidence laws

In Australia this is the Commonwealth Evidence Act, 1995

- should be regarded as ‘rules for “admissibility” of evidence including documents
Admissibility is:

- NOT a visibly identifiable quality of a document (ie like structure, etc.)
- Dependent upon many circumstances (eg the case, the nature of the business)
- NOT the same as the weight which is given it in litigation (ie an admitted document may be given no weight)
- NOT guaranteed (or ‘guaranteeable’)

What's a document under Australian law?

“Document” is defined in Part 1 of the Dictionary to the Evidence Act 1995 (Cth) as follows:

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

Further, Part 2 & 8 of the Dictionary to the Evidence Act 1995 (Cth) expands the definition of "document" by providing:

A reference in this Act to a document includes a reference to:

(a) any part of the document;
(b) any copy, reproduction or duplicate of the document or of any part of the document;
(c) any part of such a copy, reproduction or duplicate.

(Quoted in Queensland Law Reform Commission 1998: 20)

The most IS administrators can do?

- Be aware of evidential requirements
- Be aware of the kinds of issues which arise in similar organisations
- Avoid pitfalls revealed by cases where records were ruled inadmissible
Evidence Acts’ response to technological change

- Exemptions to ‘hearsay’ rules identified
- Response to replication technologies (e.g., photocopiers)
- Issues related to digitised data and electronic systems (e.g., what is the ‘original’ of an electronic document?)

The difference that electrons make

‘Electronic records also tend to be more ephemeral than paper-based records. It takes a conscious decision, and deliberate action, for an individual or agency to destroy a paper-based record.’

(AGEC 2000: 2)

The difference that electrons make

‘In an electronic environment record destruction happens automatically. The client data records maintained by an Internet Service Provider, for example, will only be kept for as long as the relevant computer program requires that they be kept.’

(AGEC 2000: 2)
Implications for information managers?

Because admissibility cannot be guaranteed, having records produced by your system ruled out is not a failing on 'your' part.

Implications for information managers?

BUT you can be held accountable if:
- The system is designed and functions poorly
- It doesn't replicate standard procedures followed everywhere else
- It takes no account of the requirements for evidence

Specific legislation 3: Privacy laws

- (Until December 2001) applied only to public sector information
  - Amended and extended in response to legislative change in EEC
- Complements FOI legislation (ie is intended to protect personal information)
- Needed to instill public confidence in information gathering/use processes
Information Privacy Principles (IPPs):

- Form the basis of various privacy acts in Australia and elsewhere
- Cover the collection, storage, access, usage requirements for personal information
- There are 11 principles in all - see the Commonwealth Privacy Act 1988 (http://www.privacy.gov.au/publications/ipp_s_print.html)

Information Privacy Principles

- Manner and purpose of collection of personal information
- Solicitation of personal information from individual concerned
- Solicitation of personal information generally
- Storage and security of personal information
- Information relating to records kept by record-keeper
- Access to records containing personal information

Information Privacy Principles

- Alteration of records containing personal information
- Record-keeper to check accuracy etc of personal information before use
- Personal information to be used only for relevant purposes
- Limits on use of personal information
- Limits on disclosure of personal information
Sample IPPs

Collection Limitation Principle:
Information needs to be collected with the subject's full awareness and the gatherer of the information must identify themselves.

Data Quality Principle
The information must be current and accurate.

Purpose Specification Principle
The subject must be informed of the purposes to which the information will be put.
Sample IPPs

Use Limitation Principle

The information can only be used for those purposes for which it was originally collected or the subject's opinion must be sought to use it for other purposes.

Sample IPPs

Security Safeguards Principle

The information must be maintained securely and third parties not given access to it.

Rethinking public policy development?

- Adams (2004) raises some interesting questions about the source and nature of knowledge used to inform public policy in Australia.
- His arguments are relevant both to broader public policy development, and the narrower matter of information policies.
- Are his arguments pertinent to the private sector too?
Rethinking public policy development?

The dominant approaches to policy formulation in a centralised bureaucracy

tend to privilege expert knowledge and management knowledge, which combine to organise (including what counts as relevant) information to meet the ‘standards’ of expertise and rationality.

(Adams 2004: 32)

Rethinking public policy development?

As a consequence,

the focus is on problems to which there need to be relatively simple policy solutions. There is no place for perpetually twisted trajectories, puzzles or paradoxes - or feelings.

(Adams 2004: 40)

Next week’s lab and tutorial exercises

Lab:
– Examine the privacy provisions of online ticket vendors

Tute:
– Take part in the tutorial paper discussion
– Develop an information security policy for an organisation
Further reading


Next week

- Laws, codes of ethics, standards etc. comprise the macro-level of the socio-legal context. (ie the dimensions that all organisations have to work within)
- They are high level examples of governance
- Next time we’ll look at ‘organisation-specific’ issues, starting with security policies