The Socio-legal Context of Recorded Information
Based upon a lecture by Robert Hartland

Overview of the next 4 lectures

- What is information policy? What is the socio-legal context in which it operates?
- What kinds of legislation are organisations obliged to observe?
- What kinds of information policies must organisations develop for their internal use?
- Some examples of organisational policy — the information management implications of security, outsourcing

Hierarchy of information policy
(adapted from Weingarten 1996: 45)

Formal policies
- Legislation: privacy acts, copyright law, freedom of information acts
- Regulation: government telecommunications regulations
- Common law: libel, slander

Informal policies
- Standards and guidelines: fair information principles for private personnel records
- Organisational rules: E-mail confidentiality in private firms, security policies
- Mores and norms: Do not read other people’s mail. Do not lie. Do not swear

What is information policy?

Weingarten (1996: 45) suggests that:
In its broadest sense, information policy is the set of rules, formal and informal, that directly restrict, encourage or otherwise shape flows of information.

Differing perspectives on public policy
(adapted from Weingarten 1996: 46)

- Free flow of information is crucial to a free society
- ‘Fair use’ is a basic part of the intellectual property bargain
- Libraries provide a critical public service
- In an information society, librarians will be increasingly valuable
- Some information is dangerous and access to it should be proscribed
- Protecting the information market will encourage creation of new information
- Other claims on tax revenues are more important
Why do you need to know any of this?

- Information systems operate within a socio-legal framework
- Questions of jurisdiction:
  - regional?
  - national?
  - global?
- Ability to liaise with lawyers

The information manager’s role

- Know that the legislation exists
- Ensure that the information is captured, maintained and available
- Consult with legal advisors as required
- Assist management with the development of avoidance strategies?

Recorded information is ...

The big picture

Recorded information and compliance 1
Recorded information and compliance 2

- The fact that records have been kept makes it possible to comply with legal and other external obligations
- Laws and external regulations increasingly dictate the form in which records must be made available for inspection

A ‘Juridical system’ encompasses:

- Statutes
- Laws
- Codes
- Standards
- Ethics

The juridical system is another name for the socio-legal system/context

The big picture

- The fact that records have been kept makes it possible to comply with legal and other external obligations
- Laws and external regulations increasingly dictate the form in which records must be made available for inspection

A ‘Juridical system’ encompasses:

more than constitutionally based legislation:
- Indigenous legal systems
- Beliefs of minority religions
- The codes and standards of particular industries, professions, associations
- And more

Eg: organisations such as the Australian Council of Churches, ISO, the Business Council of Australia, etc.
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.

Recorded information as evidence

- Has particular legal requirements for both how the courts and how the laws views evidence and how businesses use it.
- Data and documents in themselves are not evidence. E.g. a patient record needs to maintain evidence of treatment over time. BUT a hospital database of patients may serve a totally different purpose. (How many beds are vacant now? etc.)

The law is imprecise

- ‘data’, ‘information’, ‘document’ and ‘record’ can be used in a number of ways.
- Interpretations become ‘context-specific’.
- NB. The important role of precedent and Case Law in providing these ‘definitions’.

Records are part of

the governance of legal relationships, such as:
- Personal (e.g. marriage, custody, birth, wills)
- Public (e.g. tax/taxpayer, property ownership)
- Commercial (buyer/seller, customer/service provider)

But the Australian Standard (4390)

states that a record is:
‘Recorded information in any form, including data in computer systems, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs and kept as evidence of such activity.’

In records creation,

the rights and responsibilities of the following come into play:
- writer
- author (not the same as writer) or record creator
- recipient
- data subject
- third party
Eg ‘authorship’ as a legal issue

- Authentication?
- The competence or authority of the author?
- Records created in the normal course of business have more authority?
- Ownership? – author or recipient?

National Archives guidelines state ...

Key points
- Digital records can be easily modified, so their security is very important (§3).
- Australian Government agencies are required to provide adequate security for their records (§2).
- Australian Government agencies may adopt some basic practices to secure their digital records and systems (§3).
- Australian Government agencies must implement systems and procedures that prevent unauthorised alteration of digital records (§3).
- Particular care should be taken that digital records of long-term value remain authentic and accessible (§3).


FOI is commonly deemed necessary because:

- There is growing popular pressure to make governments more accountable
- The state seeks to regulate fraud and corruption
- It provides rights of access to personal information and may help ensure accuracy

Specific legislation 1: Freedom of Information

- A legally enforceable right of access to government information in documentary form
  - One’s personal ‘files’ held by government agencies
  - Operations of government agencies
- Subject to exemptions
- Applies only to government information (ie the public sector)
- Exists at both Commonwealth and state levels

What information is not available?

Exemptions include:
- Third party interests – eg documents impinging on personal privacy, business affairs information (‘commercial confidentiality’)
- Particular agencies (eg ASIO)
- National security, defence, international relations documents that would damage the state if released
- Cabinet and Executive Council documents
- Many ‘internal working documents’ (ie deliberative process documents)
<table>
<thead>
<tr>
<th>Who uses FOI? And does it work?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Individuals wishing to gain access to personal agencies</td>
</tr>
<tr>
<td>• Business organisations – for direct marketing and other purposes</td>
</tr>
<tr>
<td>• Politicians (particularly the Opposition)</td>
</tr>
<tr>
<td>• Journalists</td>
</tr>
<tr>
<td>NB. Appeal mechanisms such as Ombudsman, Administrative Appeals Tribunal, courts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is this the most IS administrators can do?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Be aware of evidential requirements</td>
</tr>
<tr>
<td>• Be aware of the kinds of issues which arise in similar organisations</td>
</tr>
<tr>
<td>• Avoid pitfalls revealed by cases where records were ruled inadmissible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specific legislation 2: Evidence Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Australia this is the Commonwealth Evidence Act, 1995</td>
</tr>
<tr>
<td>– should be regarded as ‘rules for “admissibility”’ of evidence including documents</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence Acts’ response to technological change:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has evolved in response to Common (or Case) Law decisions</td>
</tr>
<tr>
<td>• Exemptions to ‘hearsay’ rules identified</td>
</tr>
<tr>
<td>• Response to replication technologies (eg photocopiers)</td>
</tr>
<tr>
<td>• Issues related to digitised data and electronic systems (eg what is the ‘original’ of an electronic document?)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admissibility is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• NOT a visibly identifiable quality of a document. (ie like structure, etc.)</td>
</tr>
<tr>
<td>• Dependent upon many circumstances (eg the case, the nature of the business)</td>
</tr>
<tr>
<td>• NOT the same as the weight which is given it in litigation (ie an admitted document may be given no weight)</td>
</tr>
<tr>
<td>• NOT guaranteed (or ‘guaranteeable’)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implications for information managers?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Because admissibility cannot be guaranteed, having records produced by your system ruled out is not a failing on ‘your’ part</td>
</tr>
</tbody>
</table>
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

Further reading


