

Andrew Charlesworth
Director, Centre for IT & Law

Data Transparency: Managing the legislative risk

7th International Digital Curation Conference
Bristol, 5-7 December 2011.



The Broadening Spectrum of Risk

- Increasing public access to, and scrutiny of, research methodologies, processes and outputs is not without practical legal consequence.
 - Institutions must consider the implications of legal issues such as privacy, confidentiality, freedom of information and intellectual property for research/archiving practices.
 - Researchers need to be able to identify and address legal risks at an earlier stage.
 - Archivists need to obtain comprehensive and accurate legal metadata to ensure that future reuse of research data is compliant with specific legal obligations.
 - With enough eyeballs, all potential ethical and legal breaches become shallow.

Storing up Trouble

- Where research data is held for x period of time
- Who is responsible for curating that data?
- Leaving safe storage to researchers over long periods of time is problematic
 - Staff turnover and equipment replacement
 - Advances in technology/software
 - Inadequate security for personal data (DP, confidentiality)
 - Ability of institution to locate data at short notice (FOIA)
 - Ability of institution to determine when data should be weeded/deleted, and who should do it (ownership of data)
 - Loss of surrounding data, loss of context

Off the Rails

- Most legal and ethical problems arising from research data occur because of:
 - Lack of effective control (ownership/guardianship)
 - Lack of appropriate/accurate information (metadata)
 - Poor understanding of legal and ethical issues by researchers, archivists and administrators (or refusal to engage, or deliberate misinterpretation)
 - Failure to adjust policies and practices to new circumstances (law, technology, politics - evergreening)
 - Lack of sanction (where do consequences of data loss, data breach, data misuse fall?)

Seeking Solutions

- Proactive policy development and review
 - Avoiding catching today's hot potatoes with the oven gloves of yesterday
- Identifying institutional 'data guardians'
 - Allocating responsibility, knowledge, control, oversight.
- Effective metadata handling
 - Collection, adhesion, transfer, interpretation/translation
- Education, education, education.
 - Across the spectrum, including reusers of data
- Developing support systems for data transparency
 - Placing data in context, identifying problem areas/issues

Avoiding Undue 'Legalisation'

- Research data risk minimisation measures should be proportionate and context/discipline sensitive.
 - risk assessment-based rather than blanket rules.
 - issues like requirement of anonymisation of data, or of written consent, addressed on a case-by-case.
- The growth of FOI/EIR requests for research data requires an informed and measured response.
 - institutions need to be familiar with the relevant FOI/EIR exemptions, and able to justify their use where necessary
 - researchers need to be aware of the possibility of Information Requests, and prepared to deal with them