ETHICAL AND LEGAL ISSUES IN DATA SHARING - OVERVIEW

LIBBY BISHOP
UK DATA ARCHIVE
UNIVERSITY OF ESSEX

LOOKING AFTER AND MANAGING YOUR RESEARCH DATA (GOING DIGITAL AND ESRC ATN EVENTS)
UK DATA ARCHIVE, COLCHESTER, 24-25 APRIL 2013
ETHICAL AND LEGAL ISSUES IN DATA SHARING

A COMBINATION OF GAINING CONSENT FOR DATA SHARING, ANONYMISING AND REGULATING ACCESS TO DATA WILL INCREASE THE POTENTIAL FOR MAKING PEOPLE-RELATED RESEARCH DATA MORE READILY AND WIDELY AVAILABLE

AREAS OF COVERAGE

• Legal and ethical aspects
• Informed consent for data sharing (Thursday)
• Anonymising data (Thursday)
• Controlling access to data
• Working with Research Ethics Committees
ETHICAL ARGUMENTS FOR ARCHIVING DATA

- Store and protect data securely
- Not burden over-researched, vulnerable groups
- Make best use of hard-to-obtain data (e.g., elites, socially excluded, over-researched)
- Extend voices of participants
- Provide greater research transparency
- Enable fullest ethical use of rich data

In each, ethical duties to participants, peers and public may be present
DUTY OF CONFIDENTIALITY AND DATA SHARING

- Duty of confidentiality exists in common law and may apply to research data

- If participant consents to share data, then sharing does not breach confidentiality

- Public interest can override duty of confidentiality
  - May need to give up data for court subpoena or to police
  - Best practice is to avoid vague or general promises in consent forms
DATA PROTECTION ACT, 1998

- Personal data:
  - relate to living individual
  - individual can be identified from those data or from those data and other information
  - include any expression of opinion about the individual

- Requirements for handling personal data
  - processed fairly and lawfully
  - obtained and processed for a specified purpose
  - adequate, relevant and not excessive for the purpose
  - accurate
  - not kept longer than necessary
  - processed in accordance with the rights of data subjects, e.g. right to be informed about how data will be used, stored, processed, transferred, destroyed, …; right to access info and data held
  - kept secure
  - not transferred abroad without adequate protection

- Personal data can be disclosed only with consent
Exceptions for personal data collected as part of research:

- can be retained indefinitely (if needed)
- can be used for other purposes in some circumstances
- people should still be informed

If data are anonymised (personal identifiers removed) then DP laws will not apply as these no longer constitute ‘personal data’

DPA is not intended to, and does not, inhibit ethical research
SENSITIVE DATA

• Data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions (DPA 1998)

• Can only be processed for research purposes if:
  - explicit consent (ideally in writing) has been obtained; or
  - medical research by a health professional or equivalent with duty of confidentiality; or
  - analysis of racial/ethnic origins for purpose of equal opportunities monitoring; or
  - in substantial public interest and not causing substantial damage and distress
BEST PRACTICE FOR LEGAL COMPLIANCE

• Investigate early which laws apply to your data

• Do not collect personal or sensitive data if not essential to your research

• Seek advice from your research office

• Plan early in research

• If you must deal with personal or sensitive data
  • inform participants about how their data will be used
  • remember: not all research data are personal (e.g. anonymised data are not personal)
OPTIONS FOR SHARING CONFIDENTIAL DATA

- Obtain informed consent, also for data sharing and preservation / curation
- Protect identities e.g. anonymisation, not collecting personal data
- Regulate access where needed (all or part of data) e.g. by group, use, time period
- Securely store personal or sensitive data
CONSENT NEEDED ACROSS THE DATA LIFE CYCLE

- Engagement in the research process
  - decide who approves final versions of transcripts

- Dissemination in presentations, publications, the web
  - decide who approves research outputs

- Data sharing and archiving
  - consider future uses of data

Always dependent on the research context – special cases for covert research, verbal consent, etc.
REGULATING ACCESS DATA

- Essential when anonymisation ineffective or damaging to quality
  - visual or audio data
  - disclosive microdata

- UK Data Archive has gradation of access controls
  - small number of studies are open (no registration)
  - majority require registration
  - data users sign legally binding End User Licence – e.g. not identify any potentially identifiable individuals
  - stricter regulations for certain types of data:
    - Special Licences
    - Approved researchers
    - require data access authorisation from data owner prior to data release
    - embargo for given time period
    - Secure Data Service (no direct data access)

- Multiple AC can apply to different data types within one study
DATA SHARING AND RESEARCH ETHICS COMMITTEES

- RECs are responsible for safeguarding participants from harm and ensuring ethical research (and protecting home institutions), but are not (always) informed about sharing.

- There can be perceived tensions between data sharing and protection.

- UKDA tries to ensure that RECs know:
  - anonymised data are not subject to DPA
  - most funders require or encourage data to be shared
  - most research data can be shared
  - procedures (consent, anonymisation, regulating access) are available to enable ethical sharing
  - data archives ensure ethical re-use of research data, protection of participants and safeguarding of personal data.
Project 1
My research is into the pro-anorexia phenomenon. Pro-anorexia operates across websites and forums which treat anorexia nervosa as a lifestyle choice; it comprises tips, tricks, and images to inspire its users. As such it has been accused of perpetuating anorexia and is subject to deletion by internet moderators - this means my data is somewhat evasive. I need to save screen shots of the text and images I am analysing in my research.

Project 2
My current research interests are around Video Sniffing of CCTV footage. Some of my 'data' are therefore in the forms of hacked videos. Some of them can be found from Deptford.TV website (e.g. http://edit.deptford.tv/node/204 and http://edit.deptford.tv/node/209). Interested also in ethical issues that this practice might raise.