Preserving the public record vs the ‘right to be forgotten’:

policies for dealing with notice & takedown requests

Nicola Bingham
Lead Curator, Web Archiving
British Library

National Library of New Zealand

14th November 2018

Background: GDPR and DPA

- EU General Data Protection Legislation May 2018
- UK Data Protection Act May 2018

Implications for web archiving:

"a right [for the data subject] in certain circumstances to have personal data rectified, blocked, erased or destroyed"

- Consideration of archival principles, preserving the public record, vs the “right to be forgotten”
- Review of Library policies, procedures and guidelines around personal data and takedown of material

Mission and principles of Legal Deposit Libraries

- Collecting online data to preserve the nation's historical record and satisfy researcher demand for aggregated personal data.
- Libraries legal underpinning:
  - Legal Deposit non-Print works Regulations 2013
  - The British Library Act 1972
- Collection principles: Collections will be impartial, neutral, comprehensive & unfiltered.
- The Library will avoid censorship, even unintended.

Legal Deposit Libraries derogation from the “right to erasure”

Legal Deposit Libraries have derogation under the following terms:

- in order to comply with a legal obligation;
- for the performance of a task carried out in the public interest;
- and for archiving purposes.

“Taking down” material is always interpreted as suspending access rather than deletion.

Factors beyond law and regulation

- Duty to protect individuals privacy.
- Preserving the Library’s reputation with stakeholders.

Internal Risk assessment

- 2017 – 2018, Internal assessment of personal data in Collections and review of notice and takedown policies.
- Observations:
  - Web archives risky due to “scale meeting recency”
  - More potential for personal data in news & social media collections
  - Web archives are largely unfiltered and unmonitored
- Mitigation for exposure of personal data:
  - Control access to collection
  - Rapid notice and takedown policy

Internal Risk assessment: Recommendations

- Reinstate Web Archiving Steering Committee with new ToR.
- Implement a clear governance structure for review of take down policies.
- In house experts identified for escalation of difficult cases.
- Guideline document listing different scenarios and responses for front line staff.
- Review technical process to aid rapid take down of material.

Notice and Takedown Requests

- Approximately 40 takedown requests since 2013
- Generalised categories:
  - Breaches of data protection
  - Preventative takedown of potentially sensitive personal data
  - Defamation/libel
  - Copyright issues
  - Inaccurate/contested data
  - Misunderstanding of web archiving
  - General unspecified objections

Assessment and guidelines

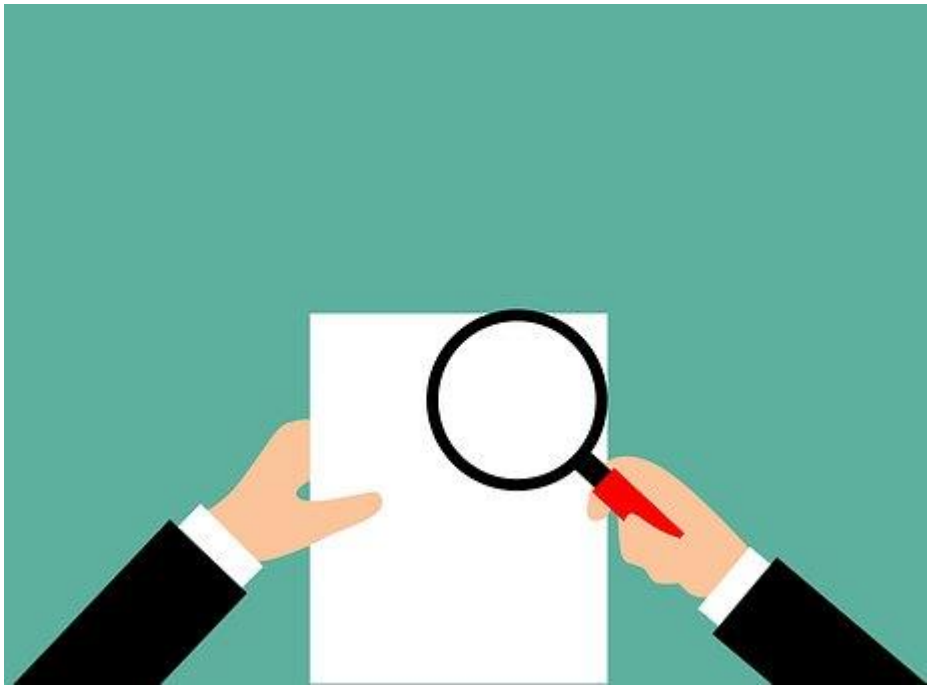
- Initial assessment against guidelines by curatorial team.
- Access may be suspended temporarily – pass URLs for blacklist from WayBack
- Risk framework and impact scores

Example: Illegal material

Scenario: We are specifically informed that a collection item contains illegal material, as identified by the court, the police or a suitable authority such as Internet Watch Foundation.			
Options **Risks:**	**Financial**	**Reputation**	**Collecting**
Do nothing and permit access to the item	R	R	G
If possible, continue permitting access but attach a notice advising that the material is illegal	R	R	G
Take down the item and permit access only on request for individual users who sign/accept an indemnity	R	R	G
Take down the item and permit access only to police or suitable authorities on application with reasonable grounds	G	G	G
Take down the item and prevent all access	G	G/A	G

Further scenarios for takedown

- **Libellous/defamatory material**
  - Take down. Possibly provide a link to court record
- **Inaccurate material/ disputed facts**
  - Generally do not take down
  - Do not take role of arbiter
  - Exceptions on grounds of health, safety & security



Copyright, database right, IP rights infringement

Libraries generally protected from copyright claims, if content archived lawfully and only available on library premises

Open access licence

- Invoked for open access content
- Intended to give protection against copyright claims

Problems with licence:

- Implies consent (can be withdrawn)
- Change in website details
- Signed by person with correct authority?
- No date range

Personal data

- No specific and legal “right to be forgotten”
- ‘Damage and substantial distress’ need interpretation
- Unlikely to takedown material if:
  - Only embarrassing, not damaging
  - Material available widely for a long period of time
  - About a publically accountable figure
  - Archived copy is the only copy
- Special consideration given to:
  - Material about children or vulnerable people
  - When privacy is a matter of security
  - Data made available without subject’s knowledge or consent
  - Material posted when suffering severe depression or mental distress

Privacy and confidential information

- Article 12 of the EU Universal Declaration of Human Rights protects the individual's privacy.
- Library does not interfere with personal privacy by web archiving.
- DCMA Guidelines definition of private data
  - Only available to a restricted group of persons
  - Works behind a barrier are still considered open
  - Private data = protected tweets to approved followers on Twitter, posts to 'friends' on Facebook, chat room discussions limited to a restricted group
  - In scope for web archiving = open access social networking pages blogs and public comments added to articles

Conclusions

- Notice and takedown guidelines help front line staff but standardised response not always appropriate.
- Recommendations:
  - Small management group to deal with difficult requests.
  - Database of takedown requests to inform policy
  - Periodic review
- Areas for further research:
  - Definition of publishing with social media
  - What is the public's expectation of privacy?

What questions do you have?