National & State Libraries Australasia

RE IMAGINING LIBRARIES

Legal Issues Discussion Paper

Updated 30 March 2015

Authors
Janice van de Velde, State Library of Victoria
Kerry Blinco, Northern Territory Library
NSLA Copyright Working Group

Introduction

This discussion paper aims to provide an overview of existing and emerging legal (and ethical) risks (such as privacy and defamation) and response options available for libraries (legal defence and risk management). The discussion paper builds on the Copyright Group's existing work to develop a standard policy position to address copyright complaints requesting the removal of online content. The information contained in this paper does not purport to cover all potential risks or provide comprehensive legal analysis, which would be beyond the expertise of the group members.

Background: impact of the law on the creation and distribution of content

As frequently stated, the digital world provides both opportunities and challenges for cultural institutions. The opportunities derive from the ability to expand access to collection materials, and enable 'real time' engagement with their communities irrespective of time and geographical boundaries. The challenges include a complex matrix of legal and ethical issues that are evolving with, and in response to, a range of factors including technological innovation, community expectations, and case law.

Copyright and privacy are critical areas of concern for their potential to limit or remove access to information. Copyright has had the most obvious impact on cultural institutions: it is the law that we are most familiar with as it includes specific exceptions that direct many operational activities. Copyright law is frequently critiqued for lagging behind technological change and failing to maintain a balance between creators and users of copyright works, and while consumers have increasingly ignored (the illogical and outdated) aspects of copyright law, cultural institutions cannot easily follow the same path.

Recent international attention on the 'right to be forgotten' represents a new challenge for cultural institutions potentially impacting on online access to digitised materials that include personal information. It follows a much-publicised privacy complaint raised against information published online in a Spanish newspaper and Google[1]

[1] The 2010 privacy complaint raised against a Spanish newspaper, Google Spain and Google Incorporated was referred to the European Union Court of Justice to test: whether or not the European Union Data Protection Directive of 1995 applied to search engines; the extent of any territorial restrictions given the location of the server; and, the circumstances for which individuals

whereby the European Court of Justice (ECJ) confirmed the validity of the 'right to be forgotten' under the European Union Data Protection directive and that this covered all the EU states (and businesses operating there) and all online publications, including social media.[2, 3] Ironically the privacy claim that sparked this debate has worked very decidedly against the individual involved as he has attained international and very public notoriety.

The rationale and ethics of this case have been debated at several levels both here and overseas. Major concerns include: the negative implications for equitable access to information (removing the link from search results has not deleted the information, which is still available, just harder to find and access); high resourcing costs (since each request must be individually assessed);[4] technological infeasibility of complete removal of information (given the multiplier effect of digital content on the web); and, the dilution of legal certainty and legitimacy (arising from the decentralisation of responsibilities from the courts to third parties).

Freedom of expression/free speech

Freedom of expression or free speech is intrinsically valued as the keystone of democracy, and formally recognised across many international jurisdictions.[5] Within the Australian context, formal recognition is limited to the *Human Rights Act 2004* ACT s 16, and *Charter of Human Rights and Responsibilities Act (Vic) 2006* while the Commonwealth

---

may have the 'right to be forgotten' and request removal of links to personal information. In this case although the Court supported the claim it also ruled that '*the right to be forgotten was not absolute but will always need to be balanced against other fundamental rights, such as freedom of expression and of the media.'* Subsequent to this ruling, the European Commission introduced a new proposal to update the 1995 Directive (the Data Protection Regulation) to ensure that: services offered by non-European companies in Europe must comply with EU rules (Article 3); the burden of proof on whether or not to maintain the data because it is still needed or relevant will fall to the data 'controller' not the data 'subject'; and the controller must make reasonable attempts to advise third parties of the deletion. The proposal outlined a number of specific reasons which would support maintaining the data online, these include: freedom of expression, public health, and historical, statistical and scientific purposes. Supporting a balanced approach, the Court advised that all assessments must be made on a case-by-case basis. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[2] Taking into account the Court's ruling the European Commission subsequently proposed a new directive to strengthen this principle to better meet the needs of the digital age, which would involve inter alia reversing the burden of proof from the individual (data subject) to the company (data controller).

[3] The Directive has not received unanimous support, the House of Lords review of the proposal made the following recommendations: *60. It is clear to us that neither the 1995 Directive, nor the Court's interpretation of the Directive, reflects the current state of communications service provision, where global access to detailed personal information has become part of the way of life. 61.* ***It is no longer reasonable or even possible for the right to privacy to allow data subjects a right to remove links to data which are accurate and lawfully available. [Emphasis added]*** *62. We agree with the Government that the 'right to be forgotten' as it is in the Commission's proposal, and a fortiori as proposed to be amended by the Parliament, must go. It is misguided in principle and unworkable in practice. 63. We recommend that the Government should ensure that the definition of "data controller" in the new Regulation is amended to clarify that the term does not include ordinary users of search engines. 64. There are strong arguments for saying that search engines should not be classed as data controllers. We find them compelling. 65.We further recommend that the Government should persevere in their stated intention of ensuring that the Regulation no longer includes any provision on the lines of the Commission's 'right to be forgotten' or the European Parliament's 'right to erasure.'*
House of Lords, European Union Committee, Second Report of Session 2014-15 EU Data Protection law: a 'right to be forgotten'? http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf p.22

[4] Apparently reassured by the fact that Google already had an established process for deletion (takedown), the Court acknowledged that it could not predict the impact of this proposal, however, just 17 days after the Court's judgement resulted Google had received 70,000 data removal requests http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f-/news/right-to-be-forgotten-report/ Google currently receives over 1,000 deletion requests per day.

[5] For example: the Constitution of the USA (First Amendment), the International Covenant on Civil and Political Rights (Article 19), European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 10), the Human Rights Act (UK) s12.

Constitution provides only a narrow freedom of political communication.[6] Freedom of speech and the free flow of information are critical ethical positions held by the library profession and are similarly reflected across international jurisdictions, the most recent being the *International Federation of Library Association's (IFLA) Lyon Declaration on Access to Information and Development*.[7] While free speech can be protected by copyright and remains an important defence to defamation, we are increasingly seeing a trend where copyright and privacy laws are being used to restrict free speech and access to information.

Obscene and indecent material

Creative outputs regarded as offensive may be subject to the laws of obscenity and indecency: these laws are designed to support access to information (for adults) while protecting minors. Galleries have typically borne the brunt of complaints relating to obscene and indecent materials: these are dealt with under common law and statute[8] and typically generate much publicity.[9] Website content is regulated through the *Broadcasting Services Amendment (Online Services) Act 1999 (Cth)* under the auspices of the Australian Communications and Media Authority (ACMA) which is responsible for issuing takedown notices and penalties to service providers.

Defamation

Defamation covers a broad range of medium: the test for defamation is not based on intent, but whether or not a reasonable member of the community understands that something conveys a defamatory meaning, and occurs at the point of access which may not be the country of origin. [10] Australia introduced uniform defamation laws in 2005: these came into effect the following year, and subsequently removed the element of privacy from defamation cases. [11]

Defences to defamation, are closely aligned to freedom of expression, and will include whether the material is: 'true or substantially true', an honest opinion, a public document, or subject to qualified privilege. [12] While these defences apply to the creator, secondary distributors of content such as libraries, will find support from the defence of 'innocent dissemination' – this defence does not apply to the *first distributor, author or originator or if there was an opportunity to exercise editorial control over the content or publication or if there was reasonable knowledge that*

---

[6] Robert Burrell and James Stellios "Copyright and Freedom of Political Communication in Australia" in Jonathan Griffiths and Uma Suthersanen (eds), *Copyright and Free Speech,* 2005 p.32

[7] IFLA http://www.lyondeclaration.org/content/pages/lyon-declaration.pdf

[8] Every state and territory has legislation restricting the exposure of people to obscene or indecent material. At the federal level, the regulation of potentially offensive materials occurs through the *Classification (Publications, Films and Computer Games) Act 1995 (Cth),* the *Customs Act 1901 (Cth)* and the *Criminal Code 1995 (Cth)*

[9] See Shane Simpson and Richard Potter, Chapter 10 "Restrictions on Freedom of Expression" *Collections Law: legal issues for Australian archives, galleries, libraries and museums.* 2011 http://www.collectionslaw.com.au/wp-content/uploads/2013/07/25-Freedom-of-Expression.pdf

[10] Marett Leiboff, *Creative Practice and the Law,* Lawbook Co. 2007 p.193

[11] The tort of defamation provides redress for a person whose reputation is damaged by a publication to a third party. Until the enactment of uniform *Acts* in 2005 in Australian states and territories, defamation law provided considerable indirect protection of private information because in some states defendants could only justify a defamatory publication by showing not only its truth but also that it was published in the public interest or for the public benefit. However, the truth of the defamatory statement is now a complete defence, so that the action provides much more limited protection of privacy. ALRC discussion paper p. 45-46

[12] Within the US context, Eric Goldman argues that web publishers can improve their defamation defences by hyperlinking to original sources: "a properly cited article, filled with hyperlinks to original source materials, should be extra-resistant to defamation claims – readers can easily inspect the source materials themselves and make their own judgements about the article's veracity." http://www.forbes.com/sites/ericgoldman/2013/01/07/top-ten-internet-law-developments-of-2012/

the matter was defamatory.'[13] Delivering an apology may also be used as a defence[14] and claims must be brought within one year from the date of publication, although this may be increased to three years.

Since the introduction of uniformity, corporations are not able to sue under defamation, an alternative option involves s52 *Trade Practices Act 1975 (Cth)* which covers misleading or deceptive conduct. Section 65A of the *Act* provides an exemption for information providers, radio and television stations, newspaper owners and others who *carry on the business* of providing information.[15] Simpson argues that there must be an argument that a collecting institution is also an 'information provider' and hence exempt.[16]

Privacy

Information privacy deals with the treatment of 'personal information' – the common element is information (or an opinion) from which an individual's identity is apparent or can be *reasonably ascertained.*[17] Privacy legislation applies not only to personal information in documents, but in images and photographs,[18] with exemptions for: g*enerally available publications;*[19] *collections of cultural institutions generally;* [20]*collections of specific institutions;* [21]*records in relation to deceased people.*

The Australian Attorney General recently received, although has yet to respond, to the Australian Law Review Commission's (ALRC) Final Report on *Serious Invasions of Privacy in the Digital Era* which considers the introduction

---

[13] Leiboff, p.217-8

[14] Simpson: *Australia's defamation laws include a procedure whereby an early apology and offer to pay costs and consideration of some monetary compensation (although this is not mandatory) may provide a full defence (regardless of other defences) if it is a reasonable offer and made within 28 days of a letter of complaint (which should state that the letter should be regarded as a 'concerns notice' under the Act). Part 3 of the 2005 Act spells out the steps which must be taken for such an offer and which must be followed carefully.*

[15] Leiboff, p. 197

[16] Simpson and Potter p.33

[17] Confidential information is defined as "information which is not generally or publicly known but is only known to a deliberately restricted number of individuals" is generally accepted that an obligation of confidence may arise where a party comes into possession of information which he or she knows, or ought to know, is confidential. This extension of the law makes the equitable action for breach of confidence a powerful legal weapon to protect individuals from the unauthorised disclosure of confidential information.
Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion Paper* DP.80 March 2014 p.46

[18] However, there is no common law right not to be photographed that can be exercised to prevent photography or filming of someone in a public place without his or her consent. [Although] Private property owners or public entities such as local councils, educational institutions or museums may regulate photography on private property or places they control, by the express terms on which entry is authorised. Australian Law Reform Commission, *Discussion Paper* p. 46-47

[19] Emily Hudson notes that: "All privacy legislation has some kind of exception for generally available information or publications. Thus a cultural institution that merely *acquires* generally available publications does not need to comply with the relevant privacy principles. That said, if the institution uses publicly available sources to *create new records* (such as entering details on a database) it may need to comply with the relevant privacy legislation." *Cultural Institutions, Law and Indigenous Knowledge: A Legal Primer on the Management of Australian Indigenous Collections,* IPRIA, University of Melbourne, 2006. p.45

[20] The Commonwealth, Victorian and Northern Territory information privacy statutes contain provisions that exempt the collections of cultural institutions from their scope. Under the Federal and Victorian legislation, the exemption relates to the purpose of the collection material which is "kept in a library, art gallery or museum for the purposes of reference, study or exhibition." In the case of the Northern Territory's legislation, the exemption also includes the availability of collection in "a library, art gallery or museum if the collection is on public exhibition or is available to the public for reference or study purposes." These exemptions are of particular relevance to manuscript and artistic collections, which may not fall within the ambit of generally available publications however due to the language used in these provisions, questions remain as to whether they apply to *restricted* collections. See Hudson p.42-47

[21] Certain specific institutions are also exempt from the ambit of privacy legislation

of a statutory tort for 'serious invasions of privacy.'[22] Privacy is regarded as a right that is in everyone's interest, although as pointed out by the ALRC, this right is a relative not absolute one and needs to reference public interest, free speech and changing community expectations about whether or not there was a 'reasonable expectation of privacy.'[23] Significantly, publically available information will not be automatically exempt; however a 'first publication rule' has been proposed to limit actions when the information has already been published.

Although the ALRC discussed the introduction of a new takedown regulatory system this was not included in its final recommendations due to the potential "chilling" impact on freedom of speech. The ALRC also argued that the ambit for claims should be limited to 'natural persons' with specified time frames,[24] and while agreeing that public interest matters such as freedom of expression and freedom of the media should be taken into account the burden of evidence for public interest falls to the defence rather than the claimant (like the EU position).

The ALRC's Discussion Paper raised the issue of the relevance of an additional Australian Privacy Principle (APP) to cover the 'deletion of personal information' contributed by that individual.[25] During the 2014 Australian Internet Governance Forum (AuIGF) held in Melbourne in August,[26] Justice Hampel SC made a number of comments on this issue, maintaining that this debate is about the 'right to erasure' or an individual's right to revoke consent, it is not directed towards rewriting the public or historical record.[27] Referencing contemporary lifestyle choices to share and contribute content through social media, Justice Hampel argued that it was important to provide individuals with a mechanism to exercise control and remove their content, which is quite different from European Court of Justice (ECJ) directive to make a third party be responsible for content regulation.

Each application must be assessed on a case by case basis – obviously a resource-intensive and time-consuming task, and given the multiplier factor associated with online information is certainly not without technological difficulties or a fool-proof guarantee that complete eradication is achievable. Information published on different formats will still be available, just harder to access.

Copyright

In the digital world, there are a number of areas where copyright infringement may impact on cultural institutions, including the digitisation of collection materials, and third party infringement arising from the use of online materials. [28] Copyright claims form the bulk of takedown claims received by NSLA libraries.

---

[22] The ALRC's attention focused on 'invasions of privacy that are serious, committed intentionally or recklessly, and that cannot be justified in the public interest …. [and] intrusion upon seclusion or by misuse of private information.' ALRC, *Serious Invasions of Privacy in the Digital Era*, Final Report 123, June 2014 p.18

[23] The 'reasonable expectation of privacy' test has been adopted by an number of jurisdictions including the USA, UK, New Zealand and Europe

[24] The limitation period is set at one year from first awareness or three years after the event, whichever comes first.

[25] The principle would: (a) require an APP [Australian Privacy Principle] entity to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual; and (b) require an APP entity to take reasonable steps in a reasonable time, to comply with such a request, subject to suitable exceptions, or provide the individual with reasons for its non-compliance. ALRC Discussion Paper p.15

[26] http://www.igf.org.au/archive-2014

[27] David Vaile, at the AuIGF 2014 suggested that Australia's spent convictions legislation, which has been effective from the early 1990s, could be regarded as a form of 'right to be forgotten'

[28] Forbes: Also notes an emerging trend where the acquisition of copyright is being used as a means to supress or control content is converting copyright law into a 'right to forget' Scott v WorldStarHipHop

A recent audit undertaken by the NSLA Copyright Working Group has revealed that copyright infringement claims are being managed largely through general disclaimers (with the aim of limiting legal responsibility) and/or copyright statements (expressing our 'good faith' intentions).[29] In contrast to higher education websites facing the same legal risks, no NSLA member has a formal published takedown policy and procedure to deal with copyright infringements.[30]

Some libraries, such as the National Library of New Zealand have a documented procedure for its *Papers Past* website however this is for internal use only. The State Library of Western Australia's *Original Materials Collection Copyright and Access Policy* briefly references takedown as a negotiation option to ensure legal compliance.[31] The State Library of Victoria does not have a takedown policy although it has recently developed an internal takedown procedure for a digitising partner responsible for copyright clearance of a specific collection.[32]

Immediate (if not permanent) takedown often eventuates from an infringement claim, as removal of content is not a preferred outcome, 'good faith' statements 'inviting' claimants to contact staff or the Library have been used to help shift the emphasis from removal to negotiation. The State of South Australia, for example, has progressively introduced this approach across a number of online platforms and channels starting with the SA memory website and most recently their YouTube site.

Culturally sensitive materials

Libraries may contain material that is considered by a cultural group to be secret, sacred or sensitive. Members of these cultural groups may request that access to this material be restricted or the item completely removed. Access may only be available to a certain group of people, or in the case of some mourning rights, be restricted for a certain amount of time.

Cultural sensitivity is contextual and it is important to identify the people with the appropriate authority to take decisions on behalf of a community about these issues. Claims may be made by well-intentioned people from outside the community on its behalf, interpreting the community needs. It will be rare that a library will be able to make takedown decisions in house. Takedown policies will most likely need to include a decision making process that includes consultation with the appropriate authority.

It is important to differentiate between material that is secret, sacred or sensitive and material that is considered culturally offensive. The ATSILIRN Protocols[33] differentiate between these two issues and describe offensive material as those that "might be racist, sexist, derogatory, abusive or offensively wrong." Libraries need to manage the tension between maintaining the historical record and responding to material that causes offense.

---

[29] An internal register of recent NSLA takedown requests suggests that the number of takedown requests are infrequent, however staff feel uncertain and exposed

[30] Australian higher education sites reviewed include: the University of Melbourne, Monash University, and the University of Western Australia.

[31] Legal compliance also governs the removal of content from the National Library of Australia's digitised newspaper collection, however in this case is restricted to false or defamatory material. http://trove.nla.gov.au/general/using-digitised-newspapers-faq/

[32] http://www.slv.vic.gov.au/victorian-historical-journal

[33] Aboriginal and Torres Strait Islander Library, Information and Resource Network (ATSILIRN) 2005. The Aboriginal and Torres Strait Islander Protocols for Libraries, Archives and Information Services. http://aiatsis.gov.au/atsilirn/protocols.php

Cultural sensitivity also applies to standards of obscenity and indecency. Standards of acceptable dress vary widely between cultures. Material that might be considered obscene in one cultural context may not in another. The existence of full or partial nudity may not in itself be sufficient determinant of obscenity.

NSLA libraries draw on a number of policies and guidelines in relation to culturally sensitive materials, including the ATSILIRN protocols and the National Library of New Zealand's *Principles for the care and preservation of Māori materials*.[34]

Issues relating to cultural sensitivity and culturally offensive takedown requests are not limited to Aboriginal and Torres Strait Islander or Māori communities.

Legal defence and risk management

Cultural institutions responding to takedown requests generally take one of two approaches. Instant removal on every occasion of a complaint or removal may be dependent on a particular trigger, which allows each institution to review the potential severity of the complaint and then decide whether or not to remove the item. The trigger response includes follow-up investigation (with legal assistance if necessary) to assess the real risk of liability: that this risk is relatively low is supported by the numerically low number of actual cases of takedown reported by institutions (as compared to an organisation such as Google).[35]

---

[34] *Principles for the care and preservation of Māori materials* are included within the National Library of New Zealand's Access Policy: http://natlib.govt.nz/files/strategy/Access_Policy.pdf

Protocol 6: Some of the materials in libraries, archives and information services are confidential or sensitive which may require certain restrictions on access for regulatory, commercial, security or community reasons. Secret or sacred or sensitive Indigenous information should not be confused with material that may be considered offensive to Aboriginal and Torres Strait Islander peoples. Guidance on the handling of potentially offensive material is provided in **Protocol 7**. Suitable management practices will depend on both the materials and the communities served by the organisations. In implementing the processes through which such materials are managed, organisations will:

6.1 Consult in the identification of such materials and the development of suitable management practices with the most appropriate representatives of the particular Aboriginal and Torres Strait Islander communities involved.

6.2 Facilitate the process of consultation and implementation by developing effective mechanisms including liaison with reference groups at local, state and national levels.

6.3 Participate in the establishment of reference groups consisting of senior library and archival services staff and Aboriginal representatives.

6.4 Seek actively to identify the existence of secret or sacred and sensitive materials by retrospectively surveying holdings and by monitoring current materials.

6.5 Each appoints specific, designated Aboriginal or Torres Strait Islander liaison officer/s to serve as the specific point/s of contact between their institution and the relevant reference group/s.

6.6 Provide suitable storage and viewing facilities with limited access as may be required.

6.7 Ensure that any conditions on access are understood by staff and users and are fully implemented.

6.8 Ensure that secret, sacred and sensitive material is managed appropriately in the Digital Environment.

Protocol 7:

Libraries, archives and information services need to recognise that their collections may contain materials that are offensive to Aboriginal and Torres Strait Islander peoples. Such materials may be racist, sexist, derogatory, abusive or offensively wrong. Many examples are of a historical nature but some are contemporary. Libraries, archives and information services have a responsibility to preserve and make accessible the documentary record but must also respond appropriately to the existence of offensive materials. Within the context of the communities they serve, organisations will:

7.1 Develop an awareness of the extent to which their collections may contain materials which will be offensive to Aboriginal and Torres Strait Islander peoples.

7.2 Take advice from and develop effective consultation strategies with Aboriginal and Torres Strait Islander peoples in relation to sensitive materials.

7.3 Develop strategies to deal appropriately with offensive materials in consultation with Aboriginal and Torres Strait Islander peoples.

Many comparable international institutions have well-developed and publicly available takedown policies and procedures, which form an essential part of an institutions overall risk management.[36] In documenting a recent project to digitise a complex archive of materials (ranging from sensitive personal data to in-copyright publications) the Wellcome Library in the UK notes that: *It should be standard practice for any type of online, publicly accessible repository to publish a takedown policy on their website: it's the simplest step in the risk mitigation process, applies to all material published on the site, and can provide some protection from complaints resulting from the publication of copyright works, sensitive personal data and obscene or defamatory material...in relation to 1.6 million images, the WL [Wellcome Library] have received only one takedown request for the digitised archive material that has been published on the website, and this request appears to have been prompted by the content of the material..."*[37]

In highlighting the importance of maintaining the historical record, the National Archives (UK) notes that 'as a general rule, information published on a website will be considered to be in the public domain and will be removed from that website only in **exceptional circumstances**, at the discretion of The National Archives.'[38]

The National Archives of Australia (NAA) has also recently researched the ethical issues and risks associated with the 'pro-active digitisation' of government records that fall within the open access period.[39] While copyright is not a major issue for the NAA, as the Commonwealth owns copyright in a large proportion of the NAA's records, its pro-active digitisation efforts do need to be balanced against the potential harm that may arise from online exposure of personal information, and any subsequent requests for redaction or takedown of records. In responding to takedown requests the NAA response will include an explanation of the Archives Act 1983 to make publicly available open period records,[40] and advise that records are checked for sensitivities before they are released. The NAA has received only a small number of takedown applications. In the current financial year (July 2014 to January 2015) 21 requests relating to the release of records containing personal information have been received: of those only 6 requests have resulted in the digital images being withheld. Reasons why only a small percentage of images have been withheld following a request most likely relate to the relationship of the complainant to the record – the person making the request must be the subject of the record or an immediate relative (child, parent, spouse or sibling), or because the complainant did not respond to the Archives requirement that they supply a signed statutory declaration to support their claim (request). [41]

While cultural institutions strive to ensure open and equitable access to information, the digital environment makes it impossible to avoid takedown complaints. At a practical level, the assessment such complaints may need to consider a number of criteria, including:

[36] Benchmark institutions: the British Library, the Bodleian Library, the National Archives, Wellcome Library, Imperial War Museum, National Library Board of Singapore, Jorum,

[37] Victoria Stobo et al, "Copyright & Risk: Scoping the Wellcome Digital Library Project" CREATe Working Paper No.10 (December 2013) p. 40 http://www.create.ac.uk/publications/wp000010

[38] The National Archives, Takedown and Reclosure Policy. http://www.nationalarchives.gov.uk/legal/takedown-policy.htm - emphasis added.

[39] National Archives Australia, *Research Paper: The ethical quandary of digitisation and reference services*, 2012.

[40] Since May 2010, the open access period for Commonwealth records as defined by the Act begins after 20 years instead of the previous 30 years.

[41] Email correspondence with the NAA

- Changed circumstances - material previously published in good faith may have acquired sensitivity through being made available online.
- The material includes personal information about someone who is still alive and continued online access would be harmful to them.[42]
- The extent to which this information is already in the public domain.
- The material is defamatory or obscene.
- The material was released in error.
- The material infringes copyright [43]

Although online material may be removed, it is important to note that this action may only be limited to an institution's website and will not be permanent. The information may still be available to the public onsite and in the longer term is likely to be reinstated as circumstances change, after the lifetime of the applicant or a specified embargo period.

Conclusion and recommendations

Digitising and providing online access to collections clearly requires institutions to make substantial investments in technical infrastructure, but it also requires a commitment to ensure that complex legal obligations and ethical issues are considered and managed through an appropriate governance framework, as well as staff training to maintain or enhance professional knowledge.

The governance framework should include policy and procedural documents to cover specific legal areas such as information privacy, copyright, sensitive materials and requests to remove links to content (takedown complaints).

The NSLA Copyright Working Group is currently developing a position statement which aims to establish a set of general principles to guide and support a consistent approach to takedown requests. In addition, the Copyright Group has begun to record takedown requests and responses on the NSLA website and it is expected that this information will assist NSLA members to provide consistent responses. Access to these details will remain password protected.

While the initial scoping for our work on takedown was restricted to copyright infringement and culturally sensitive materials we believe that it is possible to draft a statement to provide a framework that can be used to manage all requests to remove online content. This will reference professional ethics and our (general and specific) legal obligations. [44]

---

[42] The relationship of the complainant to the material is significant – the NAA, for example, will 'only act on concerns expressed by the subjects of information… If the subject is deceased and the complainant is an immediate relative and wishes to pursue the matter, [the NAA will] invite them to put their concerns in writing … The complainant will need to: explain the reason they object to the record being online including the particular information they find distressing; and provide a statutory declaration to support their claim, affirming both that the subject of the file is deceased (unless this information is contained in the record) and that they are an immediate relative. Complaints from immediate relatives will be considered on a case-by-case basis… [and] The period of withdrawal of the image or item title will be negotiated on a case-by-case basis.' National Archives of Australia – Reference Manual – 3.12, January 2011.

[43] Archives New Zealand

[44] The statement will reference jurisdictional privacy issues as legislative frameworks and principals relating to privacy and sensitive information are specific to a jurisdiction, with State and Territory legislation taking precedence over commonwealth legislation. The OAIC is also responsible for privacy functions at the commonwealth level http://www.oaic.gov.au. From 12 March 2014, the Australian Privacy Principles (APPs) replaced the previous National Privacy Principles (NPPs) and Information Privacy Principles (IPPs). This change was embodied in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, providing 15 months advance notice of the changes. The new APPs take into account the impact of technology changes on storage and transmission of data and privacy. Depending on the date of the latest legislation in a jurisdiction, privacy principles

In keeping with previous communications work undertaken by the Copyright Group, the aim of the position statement on takedown will be to provide plain English information for the public: it is envisaged that the statement will match takedown statements of comparable institutions and will reference broad information and format requirements, response options and timeframes.[45] The statement should have a reasonable level of visibility on NSLA websites (at least matching current copyright and disclaimer statements).

The Working Group suggests that operational procedures, such as deciding where responsibility for takedown decisions resides (be it a panel, committee or individual) should be determined and reflect individual institutional requirements.

NSLA libraries should also ensure that they have an effective record-keeping process to manage takedown: while many institutions may choose to use existing records management systems, NSLA may wish to review the potential use of *RefTracker* for this purpose. This proposal was raised in the NAA *Research Paper,* which suggested that: *RefTracker has the capacity to add a series of templates and actions that are specific to a takedown application [which]…would facilitate the streamlined delivery, monitoring, and evaluation of the service.*[46]

Given that the mandatory role of the NSLA libraries to collect, preserve and provide equitable access to cultural heritage information, it must be stressed that removing online content will be require staff intervention and resources as it still requires a case by case assessment based on the competing public and individual interests, and these interests will change over time.

Removal of online content or indexes to content is not a comprehensive or permanent state: unless the original collection item is discarded it will still be available offline in reading rooms and there is no guarantee that other independent online platforms will voluntarily follow suit to remove online content – it will still be available, just harder to access.[47]

---

may be more closely aligned with the older NPPs and IPPs than the newer APPs. Even when privacy legislation dates from a similar time there may be significant differences in the wording of adopted privacy principals between jurisdictions. Links to jurisdictional information can be found at http://www.oaic.gov.au/privacy/other-privacy-jurisdictions/state-and-territory-privacy-law

[45] For example, claims are to be made in writing, provide personal contact information, full details of the complaint. Response options may vary according to the nature of the complaint, however the time frame for responding to initial claims should be standardised to a workable range, for example time frame used by the National Archives of Australia is 3 working days from receipt of the complaint.

[46] National Archives of Australia p. 19

[47] Google provides two paths for information to be removed from indexes. Individuals may request removal of results directly from Google under conditions set down in its Removal Policy. https://support.google.com/webmasters/answer/1663419?hl=en&ref_topic=1724262. In most circumstances it is necessary for removal requests to be actioned by the site owner. Google supplies instructions and tools to webmasters to assist in removal of pages from indexes. Temporary removal of indexes to the page is achieved by using the webmaster URL removal tool. https://support.google.com/webmasters/answer/1663419?hl=en&ref_topic=1724262. It is critical to use the exact URL in the Google index display in the removal request, not the URL as designated by the site, in order for index entries to be successfully removed. Processing the request may take several hours, or even days. Within 90 days other actions must be taken or the page will be reindexed. https://support.google.com/webmasters/answer/6062602?hl=en Updates to the local sitemaps may also be require to prevent reindexing. These can be tested by forcing a reindex through the webmaster tools.