A Digital Lives Research Paper

Digital Lives >> Legal & Ethical Issues

Andrew Charlesworth, Centre for IT & Law, University of Bristol

DISCUSSION PAPER

14 October 2009

A discussion paper of the Digital Lives research project, led by the British Library, in partnership with University College London and the University of Bristol, and funded by the Arts and Humanities Research Council

http://www.bl.uk/digital-lives/index.html

The paper examines a range of legal and ethical issues that pertain to personal digital archives and their collection, preservation and access

Latest revision 18 September 2009; proofing, style and layout implemented and checked for release 14 October 2009

Possible citation style: Charlesworth, A. (2009) *Digital Lives >> Legal & Ethical Issues*. Digital Lives Research Paper, 14 October 2009.

All hyperlinks checked 7 October 2009

About Digital Lives

The Digital Lives Research Project is designed to provide a major pathfinding study of personal digital collections. The project team drawn from the British Library, University College London and University of Bristol is led by **Dr Jeremy Leighton John** of the British Library (the lead partner) and funded by the Arts and Humanities Research Council (AHRC), Grant Number BLRC 8669.

The research for Digital Lives commenced in September 2007 and was funded until March 2009, with dissemination ongoing. The output of the research is expected to be of significant interest within arts and humanities, and the archives, library and information science professions as well as social and human sciences. It will also be of direct relevance to individuals who wish to manage their own personal digital collections for family history, biographical or other purposes.

The paper does not necessarily reflect the official policy of the British Library.

About the Centre for IT & Law

The Centre for IT and Law at the University of Bristol is a pioneering centre dedicated to tackling the new legal challenges associated with the fast-moving world of information technology. It is a cross-disciplinary venture, building on existing strengths in the School of Law and Department of Computer Science. The Centre was established with funding from Vodafone Group Services Limited, Herbert Smith LLP, Hewlett Packard Laboratories, Barclaycard, and the Law Society Charitable Trust.

About the Author

Andrew Charlesworth is Reader in IT Law and Director of the Centre for IT & Law at the University of Bristol, where he holds a joint post in the School of Law and Department of Computer Science. His research spans a range of topics in IT law, e-commerce and intellectual property.

Digital Lives >> Legal and Ethical Issues

Contents

Executive Summary

Overview

This discussion paper aims to provide an overview of the main legal and ethical issues that pertain to the collection and preservation of, and access to, personal digital archives (hereafter PDArcs), by repositories, including the legal deposit libraries, and other non-deposit organisations. It does so by initially examining the new social and technological environment in which the creation of PDArcs is taking place. It notes that mapping existing repository practices with regard to 'high profile' personal collections, whether analogue or analogue/digital, to the wider accession of both 'high profile' and 'digital public' PDArcs, often stored across a variety of systems, is going to be problematic. The huge increase in 'user-created content' (UCC) is discussed, along with the legal issues and innovations, such as the Creative Commons, that have emerged as a direct result. The influence of the internet, and particularly Web 2.0 technologies, such as Facebook, Flickr and YouTube, is examined, and the role of commercial intermediaries and the possible strategic alliance of repositories with such commercial intermediaries to obtain mediated access to PDArcs/PDArc content is considered - as is the future role of repositories in a UCC-dominated Web 2.0 environment.

Attention then turns to discussion of the key legal issues that are likely to affect the role of repositories in collecting, preserving, and providing access to, PDArcs. These are identified as copyright, data protection and privacy law, freedom of information requirements, and content liability both civil and criminal, including defamation, and obscene/indecent materials. Each area of law is briefly summarised (with recommendations as to further detailed overviews), its application to PDArcs analysed, and primary areas of concern discussed. A pragmatic response to legal risks is recommended, with a flexible legal policy framework, based on an effective legal risk management process, premised as the key to establishing and maintaining both depositor and user trust in the reliability of a repository, and thus encouraging both deposit and reuse of PDArcs. The paper also examines the issue of ethics in the collection and preservation of, and access to, PDArcs, noting that changing public expectations about when material from deposited PDArcs will be available, and under what conditions, will require public repositories to define a clear set of ethical standards setting the normative standards for access to such materials.

In essence, the paper concludes, most of the legal and ethical issues will be identical for analogue personal collections and PDArcs. Where differences start to emerge, they do so because of:

- the range of types of PDArc that now exist because of the storage capacity of digital media, and the readily availability of tools with which to create and capture content and information for posterity;
- the involvement of commercial entities in providing the technology and support for the creation and maintenance of PDArcs;
- the ease with which digital data can be accessed, stored and copied;
- the expectations of the public about how, where and when PDArcs should be accessible, and for what purposes.

Technology frequently runs ahead of existing laws and ethical guidelines, and at least some of the solutions to the problems this can cause are likely to lie outside traditional approaches to handling legal and ethical issues.

The paper then examines a number of potential strategies/solutions that could be employed to reduce legal and ethical problems/risks. These are:

- The wider use of metadata, particularly user-generated metatagging, to incorporate legal or ethical statements about files in deposited PDArcs, with the aim of reducing both legal risk and the current ingestion time required by repositories for new PDArcs, as well as facilitating automatic determinations about whether and when material should be made publicly available. This would require:
    - a simple and easy to apply metadata schema, preferably in the form of a simple program that can generate the actual metadata from information entered into a GUI by a user;
    - basic information for would-be depositors about the purpose of metadata and its importance in the collection, archiving and making available of PDArcs;
    - the provision of incentives to encourage would-be depositors to use the metadata system.

  A side-benefit of an agreed metadata schema for PDArcs used across multiple repositories would be the possibility of greater interoperability between them.
- Greater involvement of repositories in the development of Web 2.0/UCC 'community' practices which will enhance the creation, and collection processes of PDArcs. This could take the form of:
    - provision of long term archiving access and preservation for certain types of PDArc – services which are less likely to be supported by 'free' Web 2.0 services;
    - making such services available for PDArcs that are effectively structured and filtered, and which contain basic metadata about the files within them, incentivising creators to utilise tools/processes which would facilitate deposit, and to add legal metadata.

  There is also an important role for repositories to bring clarity to the legal and ethical issues surrounding deposit of PDArcs.
- Relinquishing some of the 'gatekeeper' role, traditionally held by repositories when accessioning content, to depositors. Given that in most cases, the actual legal risks (i.e. the chance that the collection, archiving and making available of the digital object will trigger a legal action or threat of legal action) are low, it may be more cost/ time effective to simply provide guidance to those creating PDArcs on how to structure, or tag, or add metadata to their PDArc so that repositories can reduce the time spent on legal oversight during accession. This could be achieved by:
    - use of a metadata schema; or,
    - a Creative Commons-like icon system for particular risks or depositor restrictions.
- Seeking to change aspects of the legal deposit system. While this process is inevitably long-winded (e.g. the regulation generation process under the LDLA 2003), there are some legal reforms that would make a significant difference to the current legal environment in which the collection and preservation of, and access to, PDArcs occurs. Possible changes include:
    - broad application of legal deposit to a wide range of digital objects (notably those that have been made available on the web) via regulation-based harvesting and archiving;
    - provision of limited legal liability for a wider range of legal risks, where appropriate risk assessment and risk management strategies, and appropriate ethical guidelines and practices are implemented;
    - conditional delegation of legal deposit archiving powers to 'authorised' organisations, e.g. smaller archives and libraries, to collect, archive and make available digital objects.

Recommendations

Recommendation 1 – Pragmatism

Archivists should adopt a pragmatic approach to the legal risks inherent in the collection and preservation of personal digital archives.

Recommendation 2 – Risk Assessment and Policy Frameworks

Archives seeking to accession personal digital archives should have a flexible legal policy framework, based on an initial background and risk assessment, which contains clear and documented processes for deposit and access management, policy and process audit and risk amelioration, and which incorporates the ability to effect coherent change management in the light of shifts in environmental factors.

Recommendation 3 – Development of Tools and Standards

Archivists have a vital role to play in encouraging the provision of adoption of tools and standards by commercial organisations, and the adoption of those tools by the public, that will simplify the process of collection and preservation of personal digital archives, this issue requires further development.

Recommendation 4 – Strategic Partnerships

There are potential synergies in developing strategic partnerships between archives/ repositories and commercial providers of services, such as social networking services, in order to capture/ harvest digital content for archiving and future research, these should be explored.

Recommendation 5 – Information and Education in Context

If there is to be wider public interactivity with the formal archival process for personal digital archives, then archivists should consider how they deliver appropriate information about deposit and access policies, deposit agreements and metadata, pitched at the right level, to the right audience.

Recommendation 6 – Encouraging flexibility in legal protections and freedoms

There are important lessons to be learned from the Creative Commons approach to copyright that are applicable to other legal issues facing archivists.

Recommendation 7 – Publicity and Authority

Archivists must be more proactive about promoting the possibilities of their PDArc-related work to the 'digital public', and in demonstrating that their legal and ethical practices can allow them to achieve important social ends with little risk to the individual.

Recommendation 8 – Standardisation

Archivists and their umbrella organisations should consider developing and implementing, as far as possible, standardised deposit and access policies, deposit agreements and metadata standards for personal digital archive collections to aid interoperability.

Recommendation 9 – Legislative Action

Archivists and their umbrella organisations should lobby the government, and in particular the Department for Culture, Media and Sport, for an improved system of legal deposit for all digital objects made available to the public (as per s.12(5), s.13A(2) & s.13B(6) CDPA 1988), which provides archives with a clearly defined system of limited liability for accessioning and providing access to those digital objects, covering the major areas of legal risk, and subject to institutional provision of appropriate risk assessment and risk management strategies, and appropriate ethical guidelines and practices.

Recommendation 10 – Delegation of Deposit Powers

Legal Deposit libraries should be permitted to delegate their archiving powers in certain areas to other 'authorised' organisations, including smaller archives and libraries, to collect, archive and make available digital objects. Authorisation should be conditional upon the organisation in question demonstrating that they have appropriate risk assessment and risk management strategies and appropriate ethical guidelines and practices. Organisations should be subject to regular audit on these issues, by the authorising body.

Glossary

ePortfolio	"…an ePortfolio is a purposeful collection of information and digital artefacts that demonstrates development or evidences learning outcomes, skills or competencies. The process of producing an ePortfolio (writing, typing, recording etc.) usually requires the synthesis of ideas, reflection on achievements, self-awareness and forward planning; with the potential for educational, developmental or other benefits" (Cotterill 2007)
ISSP	Information Society Service Providers. This term is derived from the EU Directive on eCommerce. An ISSP is generally considered to be a broader term than Internet Service Provider (ISP) covering a wide range of services beyond Internet access provision, including online auctions (e.g. eBay) and websites containing UCC (e.g. Web sites like YouTube, MySpace and Facebook).
PDArc	Personal Digital Archive. A collection of personal digital objects composed of information and content created and assembled by individuals for their own personal purposes and reasons. It is the digital equivalent to 'personal papers'. It focuses on the personal digital objects (including websites or online storage facilities that are restricted to an individual or to family and friends). It can be contrasted with the more general notion of personal digital collections, a concept that embraces not only the personal digital archive but also those digital objects held by an individual that have effectively been published including being made widely available on the web or have been acquired from such public sources (Digital Lives project).
'high profile' PDArc	the 'traditional' personal collection, for example the papers of a well known author, or a politician. Likely to be valuable for insights into specific events, e.g. the writing of a novel, a political scandal. Usually the subject of a directly negotiated agreement between the creator (and/or their estate/heirs) and an archive or repository, as to disclosure and use (Digital Lives project).
'digital public' PDArc	a personal collection obtained from a member of the public. Likely to be valuable for insights into wider social events. May be the subject of a direct agreement between the creator (and/or their estate/heirs) and an archive or repository, as to disclosure and use, but might also be collected subject to a standard deposit agreement, or potentially, in the future, under an agreement with a commercial entity such as a social networking site (Digital Lives project).
UCC	User-created content. Also known as consumer-generated media or User-generated content. Material created by an individual or individuals, usually initially non-commercial in intent. Refers primarily to digital material placed on websites and web services, e.g. blog posts, comments on interactive websites, material such as photographs and videos uploaded to Web 2.0 services etc.

1. Introduction

> *Unless individuals are given the tools to preserve their own digital collections, future historians will have only secondary sources like textbooks and newspapers to tell them about the past. Our sense of history will be spotty, flat, biased, and unverifiable.*
>
> [from the The Rogue Librarian blog, **formerly** at <roguelibrarian.com>]

A teenager uploads her photographs from a party to Facebook to show to her friends.[1] A new parent creates a webpage to celebrate the birth of their baby girl, with photos of the child and of the gifts received, and scans of cards and letters of congratulation. An author collects and stores her e-mail correspondence on her computer, along with the digital notes and rough drafts of her short stories. A student adds a file on her career plans and goals to an ePortfolio system. A young filmmaker creates short films about his home city and posts them on YouTube. A computer scientist runs a project to capture a wide range of electronic data about his life, recording his surroundings and interactions via 'always-on video', collecting his varied digital communications (blogging, twitters, e-mails, texts, phonecalls etc.), scanning his paper-based interactions (letters, faxes, notes) and saving all his other digital outputs, (notes, photos, papers, draft chapters etc.).[2] Each of these people is a small part of the explosion of digital content that is being continuously created (and sometimes destroyed) every day.

The fetters of 'storage space' have largely been broken by the exponential growth in the capacity of digital storage media and the plunging cost per megabyte. The 40 megabyte hard disk drive of a PC in 1991 cost roughly £5 per megabyte; the 1 terabyte (technically, 931 GB of actual storage space) external drive that may hold a user's data today cost £160 in 2007, and similar drives today cost about £80. The same £5 today (leaving aside inflation) will now buy a user 58 188 megabytes.[3] Even given the burgeoning size of computer programs and their output files, this change in accessibility to storage has major implications for the types of digital information individuals and organisations can store, and for how long they can store it.

The US Internet Archive, which has as its goal 'offering permanent access for researchers, historians, and scholars to historical collections that exist in digital format'[4] stores its data, including 'texts, audio, moving images, and software as well as archived web pages', in Petabox rack systems originally created to safely store and process one petabyte (a million gigabytes) of information. As of 2009 the web archiving part of the Internet Archive - The Wayback Machine – reportedly held nearly three petabytes of data and was growing at about 100 terabytes of data per

---

1 In October 2008, it was reported that Facebook users had uploaded 10 billion photographs to the site, that 2-3 Terabytes of photos are being uploaded every day and that Facebook has just over one petabyte of photo storage. http://www.facebook.com/note.php?note_id=30695603919

2 Gemmell, J. Bell, G. & Lueder, R. (2006) MyLifeBits: a personal database for everything. *Communications of the ACM* 49(1): 88-95; Bell, G. & Gemmell, J. (2009) *Total Recall: How the E-Memory Revolution Will Change Everything*, Boston: Dutton. Also http://research.microsoft.com/en-us/projects/mylifebits/

3 For an interesting overview of the decline in price of digital storage, see http://www.alts.net/ns1625/winchest.html

4 The Internet Archive http://www.archive.org/about/about.php

month.[5] In practice therefore, the scope of the digital material which can now be created or collected by individuals and organisations, and then retained, is vast.[6]

This increasing ability to retain digital data over long periods raises a wide range of questions, both for individuals creating personal digital archives (PDArcs), and for organisations, whether publicly funded and commercial, that seek to host and archive such collections. This research paper is concerned primarily with the legal and ethical implications arising from the retention and potential future use of PDArcs by third parties. It will examine, in a broad brush fashion, how existing UK law has been, and is being, applied to the collection and retention of digital works generally. It will also consider how the ethical position regarding the creation, archiving and use of personal collections has become less clear-cut as norms about information creation, transfer and use have been influenced by public perceptions of the benefit and value of sharing.

What is clear is that there is potential for collision between the law and public expectations in several areas, notably those of intellectual property, and privacy and confidentiality. Archives and repositories will need to consider strategies to avoid becoming embroiled in legal actions, and to steer a path between public expectation and private opprobrium. This paper will endeavour to suggest some strategies for addressing both legal and ethical issues, within a pragmatic framework that permits repositories the widest opportunity to exploit the growth of the PDArc, whilst respecting those public values that both laws and ethical principles have attempted, if not always successfully, to protect.

1.1 Law and Ethics from Analogue Days

It is perhaps a truism that legal systems have struggled with the issues emerging from digital technologies; they must address not only the technical aspects of those technologies – the perfect digital copies, the speed of transmission of those copies, the reach of those transmissions – but also the social and economic aspects – not least the ability of the individual to engage in activities that once would have been the sole remit of publishing houses, media outlets, corporations and governments.

As the cast of actors in the digital environment has changed, so legal systems and those who create and shape them (legislators, regulators, judiciary etc.) have found it harder to apply meaningfully laws that were designed for a different (and smaller) set of actors working in a different (and more controllable) environment. Equally, the public have become impatient with the barriers that the law places (often to the layperson in an apparently arbitrary fashion) in the way of their desire to create, reuse, share and access digital content.

In the UK (as elsewhere), pressure from established right holders in the copyright arena has complicated matters, as new legislation has been adopted to protect their interests.[7] In the area of privacy and confidentiality, the UK legal system has been faced with reconciling the demands of high profile plaintiffs for 'privacy' (by which they may mean 'control over press coverage' or 'control over the use of my image' as much as any deeper sense of privacy implied in the phrase

---

5 Mearian, L. (2009) Internet Archive to unveil massive Wayback Machine data center. *Computerworld*, 19 March http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=hardware&articleId=9130081&taxonomyId=12&intsrc=kc_top

6 I use the word 'retained' rather than 'preserved' largely because, at present, there is no often real guarantee of preservation of stored digital data – data formats change, software and hardware become obsolete, and digital storage media have their own decay problems. See Rothenberg, J. (1999) Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation. A Report to the Council on Library and Information Resources http://eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/17/3d/34.pdf

7 See, for example, the UK *Copyright and Related Rights Regulations 2003* http://www.opsi.gov.uk/si/si2003/20032498.htm

'the right to be let alone'),[8] with the need to provide context-sensitive privacy and data protection for the general public. This task has been complicated by the use of blunt legislative instruments, such as the Data Protection Act 1998,[9] and the countervailing need not to stifle freedom of expression.

As community moral and ethical standards shift, the acceptability of making publicly available personal digital content that might once have been considered highly private has also changed. What might have been barred by law, or by social norms, may no longer be so. Over time, the law may need to reflect these changes, either by relaxing legal restrictions on the creation, transfer or use of such content; or by more explicitly stating the types of content that should remain ' beyond the pale'. The development of a 'reality TV' culture – whose leading exemplar, Endemol's *Big Brother,* explicitly underlines in its title the paradigmatic shift entailed - may also mean that legal understandings of the contexts in which individuals are likely to want, or expect, privacy, are no longer based on widely-shared community norms, but upon a fragmentary set of the whole.[10]

1.2 The Rise and Rise of User-Created Content

While personal content collections are not a new phenomenon, forming, as they do, a significant portion of many museum and archive collections, the digital medium permits the development of individual content collections on a scale, and of an information richness, hitherto unavailable to all but the professional or the wealthy. It also allows, and indeed with Web 2.0 technologies, actively encourages, the public dissemination of such collections – a photograph album becomes a Flickr page,[11] a diary becomes a blog or Facebook entry,[12] the video of a personal event becomes a YouTube upload.[13]

The rise of digital user-created content (UCC)[14] thus has several key impacts. One current effect is that 'amateur' UCC has begun, in certain areas, to edge out 'professional' content; this appears to be the case with areas of the professional photography market. Those previously in the market for 'professional' content may now seek out content which, while perhaps not of the same quality, is adequate for the task in hand. It would seem that, if this trend continues, it will inevitably have implications for the continuing production and availability of professional content and archives.[15] It may perhaps mean that in the future there will be fewer professional, highly structured and permanent archives, and an increasing range of less structured and potentially evanescent collections of UCC.

---

8 See, for example, *Campbell v MGN* [2004] UKHL 2; *Sir Elton John v. Associated Newspapers* [2006] EWHC 1611; *Prince of Wales v Associated Newspapers* [2006] EWCA Civ 1776; *Douglas & Ors v. Hello! Ltd & Ors* [2007] UKHL 21; *Murray (by his litigation friends) v Express Newspapers plc* [2007] EWHC 1908

9 *The Data Protection Act 1998*
http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

10 Calvert, C. (2000). *Voyeur Nation: Media, Privacy, and Peering in Modern Culture*. Boulder CO: Westview Press

11 Flickr
http://www.flickr.com/

12 Facebook
http://www.facebook.com/

13 YouTube
http://uk.youtube.com/

14 OECD. (2007). *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking*
http://213.253.134.43/oecd/pdfs/browseit/9307031E.PDF

15 *Ibid* at 61

It is also evident that the line between 'public' and 'private' UCC has become increasingly blurred, not least because many of those placing UCC online do so under conditions where they are unaware of, or unconcerned about, the extent to which their content is publicly available. Thus, individuals may place UCC on Facebook pages for viewing by their immediate circle of family and friends, but because they have not adjusted the privacy settings on their account appropriately (or indeed at all), the content is available to a much wider audience, or indeed the world.[16]

The growth of UCC, and the lack of clarity surrounding a particular piece, or set, of UCC's potential/intended audience, possible uses and long term accessibility, has resulted in an increasingly confused legal environment. In such circumstances, the motives, aims and objectives of those creating UCC are opaque to those wishing to use, reuse, collect, archive and make that material available to others in the longer term. When undertaking such activities with 'professional' content or small amounts of UCC, such as an author's private papers, the legal boundaries can usually be clearly defined, often by formal contract or agreement which has been preceded, if necessary, by a period of negotiation. When dealing with large amounts of UCC, and indeed with very large digital collections derived from an individual, those legal boundaries may be rather less clear, and thus the ability to discuss/negotiate acceptable legal outcomes in any meaningful fashion, using existing laws or accepted protocols, becomes limited or non-existent.

1.3 User-Created Content and Legal Trends

In response to the legal difficulties posed by UCC, a range of approaches have begun to emerge which aim to simplify the processes of use, reuse, collection, archiving and making available to others. Some have emerged from UCC communities, and have as their primary goals the simplification of legal formalities, and/or the reduction of legal barriers to sharing. Examples of these would include the Creative Commons movement, which seeks to enhance the use and reuse of copyright materials by providing a simple set of readily recognisable licences that both limit the degree of control that a copyright holder is ordinarily granted by copyright law, and clearly identify how a copyright work can be used;[17] and the Open Access movement, which while primarily concerned with access to research articles published in peer-reviewed journals, nonetheless demonstrates another technique for enhancing sharing.[18]

Some repositories have themselves also become more open in their attitudes towards collecting of UCC. Rather than simply collecting/archiving/making available material for which they have a clear formal contract or agreement, which would inevitably reduce the amount of material that they could collect, or indeed formally process, they simply accept or harvest as much material as possible, with relatively few accession constraints. Examples of these would be the commercial online service providers such as YouTube (video) and Flickr (digital photographs), and the non-commercial online Internet Archive's Wayback Machine. These online services may involve some limited upfront filtering of material, e.g. the webpage material collected for the Internet Archive does not include material from websites which exclude its 'spidering' software by use of the 'robots.txt protocol';[19] but in general their approach to legal issues is almost entirely reactive. This means that those uploading material to YouTube and Flickr are required to agree to Terms of Service which place the onus on them to ensure that the material can be lawfully placed in the service:

---

16 *Ibid* at 95

17 Creative Commons
http://creativecommons.org/

18 JISC Open Access Briefing Paper (v.2)
http://www.jisc.ac.uk/publications/publications/pub_openaccess_v2.aspx

19 A convention to prevent cooperating web spiders and other web robots from accessing all or part of a website which is otherwise publicly viewable. http://en.wikipedia.org/wiki/Robots.txt

> *This means that you, and not Yahoo! are entirely responsible for all Content that you upload, post, email or otherwise transmit via the Service.* (Flickr)
>
> *Do not upload any TV shows, music videos, music concerts or commercials without permission unless they consist entirely of content you created yourself.* (YouTube)

The repositories then respond to claims by users, or by rightsholders and others, that material has been unlawfully placed on their service by users, on a 'notice and takedown' basis. That is, if a complaint is made bringing particular material to the attention of the archive/repository, that material may be removed either permanently, or pending further investigation into its legal status. This approach has significant advantages in that the vast majority of material deposited will not be the source of complaints, and the minority of material that is can be relatively easily and quickly dealt with. The approach does carry some legal risks, however, and is most popular in the US, where online services are provided with a degree of immunity from liability by s.230(c)(1) *Communications Decency Act of 1996*. It seems unlikely that the immunities provided to Information Society Service Providers (ISSPs) within the European Union under the EU *Electronic Commerce Directive* for mere conduit, caching and hosting will extend as far.[20]

When compared to copyright, privacy appears to have been very much a poor relation in terms of the degree of consideration given to it in regard to UCC. This may be because, in the online environment, the drive towards sharing UCC has come from the US, which currently has relatively limited privacy and data protection laws, and which has shown no great interest in expanding existing laws or developing new ones.[21] Even in the EU, where privacy and data protection laws carry more weight, their application to UCC has been slight.[22] In large measure, this has been because those laws and data protection law in particular, are not, and were not intended to be, aimed at UCC, but at privacy threats of a higher level, such as corporate or governmental invasions of privacy and misuses of personal data. There is no doubt that UCC can, and does, have negative privacy and data protection implications for individuals; and that those personal risks are potentially increased by virtue of the increasing accessibility of digital content.[23] However, public perceptions of those privacy and data protection risks appear highly contextual, in that considerable amounts of personal data are made widely public in a variety of UCC, including blog entries, videos, photographs etc. that individuals might be more wary about providing in other contexts, such as formal documentation. For example:

> Anecdotal reports and studies have suggested that many profile owners display personal information about relationships, sexual behaviors, health risk behaviors such as substance use, and mental health concerns such as depression on their publicly available Web profiles.[24]

---

20 *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* (Electronic Commerce Directive) Articles 12-14, transposed into UK law as *The Electronic Commerce (EC Directive) Regulations 2002*, s.17-19. See e.g. Goldstone R. & Gill, J. Web Site Operators & Liability for UGC - Facing up to Reality? *Society for Computers & Law*, 31 Dec 2008
http://www.scl.org/site.aspx?i=ed9981

21 See, further, Charlesworth, A. (2000). Clash of the Data Titans: US and EU Data Privacy Regulation. *European Public Law* 6: 253-274; Nijhawan, D. R. (2003). The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States. *Vanderbilt Law Review* 56(3): 939-976

22 But see Case C-101/01 (Reference for a preliminary ruling from the Göta hovrätt): *Bodil Lindqvist*, OJ 2004 C7/3, where the ECJ held that there was nothing in the Directive which prevented Swedish data protection law being applied to personal webpages

23 See e.g. Gross, R., Acquisti, A. & H. John Heinz, I. (2005). Information revelation and privacy in online social networks. In: *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*. pp. 71-80. Alexandria, VA, USA: ACM

24 Moreno, M. A., Fost, N. C. & Christakis, D. A. (2008). Research Ethics in the MySpace Era. *Pediatrics* 121 (1): 157-161; also Hinduja, S. & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence* 31(1): 125-146

It is currently difficult to assess how the legal trends with regard to UCC will affect the ability of repositories to collect, archive and make available PDArcs, largely because the area remains in flux.[25] The primary area of copyright remains unsettled, not least due to the concern of commercial rightsholders to ensure that their interests are protected to the fullest extent possible, regardless of the knock-on effects of such actions in other areas of activity. While the Creative Commons has received a great deal of publicity, it is unclear to what extent its copyright licensing system has been taken up by the general public, or the extent to which non-expert users of the licensing system truly understand the practical implications of the licenses they are creating. Users may not understand that they are in fact creating a copyright licence, the extent of the permissions they are granting, or that the Creative Commons Licence only deals with copyright, and not issues such as privacy.

Take, for example, a recent US case where a photograph of a minor, Alison Chang, was posted on Flickr under a Creative Commons Attribution 2.0 license. The photograph was then used by Virgin Australia in an advertising campaign. Alison Chang's parents brought suit, claiming that Virgin violated their daughter's right to privacy by using a photograph of her for commercial purposes without her or her parents' permission. The photographer also sued on the grounds that the Creative Commons failed "to adequately educate and warn him ... of the meaning of commercial use and the ramifications and effects of entering into a license allowing such use."[26] While the claims against the Creative Commons Corporation were later withdrawn,[27] and the case against Virgin Australia in the US courts dismissed for lack of jurisdiction,[28] the case demonstrates both the lack of understanding of the purpose of a Creative Commons licence on the part of users, and the legal uncertainties still facing third parties seeking to use Creative Commons-licensed materials

© Justin Ho-Wee Wong

Equally, the position of online repositories, both public and their commercial equivalent, remains uncertain. Whilst there is support for the 'notice and takedown' approach, the activities of some online service providers, e.g. YouTube, are attracting increasing attention from commercial rightsholders who feel that such an approach does not adequately protect their intellectual property.[29] Successful legal attempts to rein in the use of 'notice and takedown' practices in dealing with commercial content would inevitably have an effect upon the collection, archiving and making available of UCC, as commercial online service providers would then become more risk averse.

The law relating to privacy and data protection is equally unsettled, although this is primarily due to two factors: first, the issues have simply not been explored to the same degree as those of copyright, where commercial rightsholders have a clear interest in clarifying the legal position; and, second, neither the UK Courts nor Parliament appears willing to take on the task of creating a

---

25 See e.g. Kennedy, R. (2009) The Risks of User-Supplied Content Online, in Barry et al, *Information Systems Development: Challenges in Practice, Theory, and Education* v. 2 Springer: 11-20

26 Lawsuit Against Virgin Mobile and Creative Commons – FAQ http://creativecommons.org/weblog/entry/7680

27 Creative Commons Voluntarily Dismissed from Lawsuit http://creativecommons.org/press-releases/entry/7865

28 *Chang v. Virgin Mobile USA*, LLC, 2009 WL 111570 (N.D.Tex. January 16, 2009)

29 See *The Football Association Premier League Limited, et. al. v. YouTube, Inc., et al* http://www.youtubeclassaction.com/

common law or statutory law of privacy.[30] In large part this is because privacy is a rather nebulous concept to pin down, and whatever definition the courts or Parliament might adopt would be likely to face significant criticism – additionally, the courts do not want to be accused of usurping the role of Parliament by creating new law. As such, changes to UK privacy law have been developing slowly and incrementally, driven, in the main, by judgments of the European Court of Human Rights. Politically speaking, this is a more acceptable approach for the Executive, as it permits legal change to occur, whilst allowing any blame for unpopular decisions to be placed elsewhere.

1.4 Commercial Exploitation of User-Created Content

As may perhaps have become apparent in the foregoing discussion, digital UCC is currently attracting commercial interest to an extent that personal analogue UCC never achieved. There are a number of reasons for this:

- digital UCC is more easily and cheaply created and disseminated than non-digital UCC, thus there is a large body of it potentially available for exploitation;
- even with vastly expanded digital storage, users want readily accessible storage – photographs are more widely accessible on a photo-sharing service, such as Flickr, than they are on a user's computer hard disk drive; and they want backup – a photograph collection is (it is sometimes claimed) less vulnerable to loss or damage on a photo-sharing service than on a user's computer hard disk drive;
- digital UCC that is readily shareable and capable of use and reuse by third parties (whether legally or illegally) is of higher value to those third parties than analogue UCC which is harder to utilise effectively;
- to many commercial players in the online environment, UCC is a means rather than an end: that is the aim is not to generate revenues from UCC itself, but rather to use large aggregations of UCC to draw in user traffic for other services, such as advertising.[31]

These factors inevitably influence the way in which commercial storage and holding service providers approach the collection, archiving, preservation and accessibility of UCC. For example:

- Commercial online service providers are less likely to require a formal approach to collection:
  - losing content is not important if there is a constant stream of replacement content, thus voluntary withdrawal of content by a depositor, or forced withdrawal due to threat of legal action by third parties, can be tolerated;
  - the authenticity of content or creator is not an issue, unless this involves the threat of legal action by third parties (at which point the service provider will, most likely, simply remove the content), as commercial online service providers are not holding themselves out as providing authenticated materials;
  - the context of the content is not an issue, nor is the accuracy of its metadata - unverified metadata may be added to content by depositors or by later users (e.g. by tagging, or backtracks).
- Commercial online service providers are likely to be more risk tolerant:
  - an organisation developing a commercial revenue stream from UCC is more likely to factor legal risks into their business equation – occasionally getting sued may simply be seen as a 'cost of doing business';

---

30 See, Wacks, Raymond. (2006) "Why There Will Never Be an English Common Law Privacy Tort." in *New Dimensions in Privacy Law*, edited by A. T. Kenyon and M. Richardson, Cambridge: Cambridge University Press, 154-83 and *The Government's Response to the Fifth Report of the Culture, Media and Sport Select Committee on 'Privacy and Media Intrusion'* (HC 458) Session 2002-2003

31 Consider Google's purchase of YouTube in October 2006 for $1.65 billion in stock. Although this now appears to have been a significant overvaluation of YouTube, it is clear that the primary reason for purchasing the company was to gain access to a larger portion of the UCC 'marketplace', potential copyright headaches notwithstanding http://news.bbc.co.uk/1/hi/business/6034577.stm

- commercial online service providers offering storage or holding services are more likely to be single focus organisations than public repositories, which may have to finance a range of activities, all of which may thus be adversely affected by the raising of risks in one area;
- there is likely to be less significant 'reputational' risk for a commercial organisation than for public repositories in involvement in threatened or actual legal actions.

- Commercial online service providers are about maximising revenue generation:
  - content is only important as long as it adds to the bottom line, there is no rational reason to retain content which does not, or is not likely to, do so; and, in the absence of specific contractual provisions with users, no legal obligation requiring retention;
  - preservation of digital content is time and resource intensive (e.g. updating obsolete software/file formats), and is likely to be of uncertain cost/benefit to a commercial entity;
  - inactive user accounts containing PDArcs are likely to be seen as inefficient use of resource, and are likely to be disposed of in the medium to long term.

It would be fair to say that the commercial online service providers offering storage and holding functionalities have, largely by trial and error, both exposed the legal problems raised by UCC and PDArcs, in areas such as copyright and privacy law, and encouraged greater acceptance of alternative strategies for coping with those legal problems. They have also been partly responsible for, temporarily at least, helping to change the way individuals perceive the ethical issues around the use, reuse and sharing of UCC – both in encouraging sharing, and in shaping the privacy norms around the exchange of content in favour of disclosure. Whether this state of affairs will continue remains to be seen - public reaction to direct commercial exploitation of UCC may yet see a retreat from both the Creative Commons, and the generally relaxed attitude towards privacy issues in UCC, if the public begin to perceive (rightly or wrongly) that they are being unduly taken advantage of.

In any event, if commercial online service providers have begun to address some of the legal and ethical questions surrounding UCC and PDArcs, but are unlikely (unless some plausible way of monetarising the role can be found) to replace public repositories as long term providers of archiving and preservation of, and access to, UCC and PDArcs, this begs several questions: what role should public repositories have, how will that role influence the legal and ethical issues that they will face, and how should those legal and ethical issues be approached?

1.5 Outlining a Role for Public Archives and Repositories

When looking at the role for public repositories in the area of PDArcs, some lessons can perhaps be drawn from the area of web archiving.[32] There, decisions had to be made about the extent of the archiving that could be feasibly undertaken, and a risk analysis carried out as regards the legal implications of archiving certain types of material. Very few, if any, public repositories were willing to undertake archiving on the scale envisaged by the US Internet Archive. Most aimed to archive key websites such as websites set up for particular events, or websites of particular interest, and to take 'snapshots' of other web content as appropriate. Most, having undertaken a risk assessment, chose to archive websites in depth only with the permission of the site owner and appropriate rightsholders.[33] These approaches considerably reduced the legal risks that those archives faced, but at the expense of the coverage they could obtain:

---

[32] See Charlesworth, A. (2003) Legal Issues relating to the archiving of internet resources in the UK, EU, USA and Australia, a study undertaken for the JISC and Wellcome Trust http://www.jisc.ac.uk/uploaded_documents/archiving_legal.pdf

Also, Beunen, A. & Schiphof, T. (2006) *Legal aspects of web archiving from a Dutch perspective*. Report commissioned by the Dutch National Library

[33] See, for example, the UK Web Archiving Consortium (UKWAC) http://www.webarchive.org.uk/

> [The UK Web Archiving Consortium] operated on a rights-cleared basis, seeking copyright permission in writing from the Web site rights holders before archiving their material. Once permission had been granted, the Web site was added to the list of resources to be harvested and gathered periodically thereafter. Rights holders also gave permission to make their archived content available to all Web users; thus, the archive provides free networked access, which is a significant benefit for researchers. However, the process of obtaining permission proved to be a large administrative burden: resource constraints meant that libraries could only ever select and approach a tiny proportion—less than 0.5%—of rights holders within the UK Web space, a space consisting of more than 6,900,000 domains and growing by some 13% annually. Responding to permission requests can also be onerous for the rights holder, especially if third-party rights must also be cleared, and many do not feel there is sufficient incentive for them to do so: of 8,114 requests made by the British Library up to June 2008, permission was successfully obtained in only 2,090 cases. Just 54 refused, but most simply failed to respond …[34]

However, similar approaches may be considered by some public repositories as appropriate to adopt for personal digital archives, according to their tolerance of risk. In the analogue environment, archives and repositories tended to concentrate on the personal collections of individuals who were of particular interest within a particular field, e.g. authors, scientists, politicians, and local worthies. These collections contained materials such as personal correspondence, legal and financial papers, personal and family papers, drafts of publications, publications etc. It is probable that such collections will remain a significant part of any PDArc process, and that the types of arrangement made with depositors or their families will remain similar in scope.

However, simply maintaining this approach to PDArcs would ignore an increasing amount of material of interest held by personal digital archives in private collections that are not known to public repositories, as well as material stored in a wide range of commercial entities offering a similar service. Unlike analogue materials, these materials currently appear to have a relatively short life span during which they can effectively be collected, whether due to changes in file formats, or in hardware. A bundle of letters from the Great War might survive in an trunk in an attic for 90 years, and still be readable and sufficiently stable to be stored indefinitely (with care) in a repository; material stored on a hard disk drive today or on a social networking site tomorrow may well be at greater risk of being lost forever.[35]

An important role for public archives and repositories is therefore going to be to:

- establish how to promote the concept of capture and preservation of PDArcs with the aim of future deposit from a wider selection of potential depositors, including provision of advice on legal issues;
- obtain access to material in commercial archives and repositories with the aim of collecting UCC and PDArcs from those sources; this will require involving the commercial archives and repositories in the process of deposit, including, again, provision of advice on legal issues.

When evaluating the case for the collection of a wider range of PDArcs, it seems reasonable to suggest that public archives and repositories might now consider being more insistent than has been the case with web archiving. The pragmatic approach taken by both commercial web archives and by Web 2.0 commercial online service providers suggests that, legally at least, the risks inherent in the collection, preservation and provision of access to PDArcs are actually relatively low, if basic risk amelioration strategies are followed.

---

34 Gibby, R. & Green, A. (2008) Electronic Legal Deposit in the United Kingdom. *New Review of Academic Librarianship*, 14 (1 & 2): 55-70 at 62

35 Consider the case of the BBC Domesday Book Videodisks: Darlington, J. Finney, A. & Pearce, A. (2003) Domesday Redux: The rescue of the BBC Domesday Project videodiscs. *Ariadne* 36 http://www.ariadne.ac.uk/issue36/tna/

But note that one of the BBC Domesday Book's creators blames the near loss of the data on "inadequate procedures for effective national curation and conservation of information assets." Mike Tibbetts, Email to the *Risks Digest Forum*, 4 November 2008 http://catless.ncl.ac.uk/Risks/25.44.html#subj7

2. Personal Digital Archives and the Law

Personal collections can be a potential minefield of legal issues, for example, while a person in receipt of a letter may own the physical letter, they do not own the copyright in the words of the letter, so a person in receipt of extended correspondence with Tony Blair or Margaret Thatcher might deposit the letters as part of their personal archive, but cannot assign, or licence copyright, in those letters, because that copyright belongs to Tony Blair or Margaret Thatcher, and eventually to his or her estate or heirs.[36]

Where the personal archive contains personal data relating to living individuals, there are likely to be data protection issues to consider, even where the depositor of the personal collection is dead.[37] Where the personal archive is held by a public authority, there may be an obligation to disclose information from it, in the absence of, for example, a clear requirement of confidentiality on the part of the depositor.[38] Statements in personal archives may be defamatory, and thus if made public before the death of the person defamed, could result in a defamation action.[39] Similarly, materials in personal archives may include information received in confidence by the collector, including material which is commercially confidential. In rare cases, materials which are relevant to ongoing court cases may be deposited, disclosure of which before cases were decided would expose archives to action for contempt of court.[40]

Often collections are deposited after the death of the collector, and frequently with conditions attached regarding access to the collections, notably temporal restrictions. Most of these issues apply, of course, to analogue personal archives too.

In the majority of cases, the person who is responsible for creating the personal collection will not have given a great deal of thought to the legal issues while creating their collection. Although some guidance has been prepared for would-be depositors,[41] it seems unlikely that this will have seen widespread circulation.[42] Archives and repositories seeking to accession PDArcs will thus be faced with a number of potential legal issues for which they will have to:

- assess the risk, drawing both upon knowledge derived from their own experience of the collection of, and provision of access to, analogue materials; and from the strategies being adopted by other organisations involved in the hosting of and provision of access to digital materials, such as ISPs;

---

36 For an example of how copyright may be used to block use of works such as letters, see Max, D. T. The Injustice Collector: Is James Joyce's grandson suppressing scholarship? *The New Yorker*. June 19, 2006 http://www.newyorker.com/archive/2006/06/19/060619fa_fact

37 Although the *Data Protection Act 1998* does not apply to personal archives while they remain in the creator's possession, it comes into force once custody is transferred to a public repository, see s.36 DPA 1998

38 See the UK *Freedom of Information Act 2000*, s.41 http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

39 Mercado-Kierkegaard, S. (2006) Blogs, lies and the doocing: The next hotbed of litigation? *Computer Law & Security Report* 22(2): 127-136

40 This is more likely to affect organisations hosting contemporary online digital material, such as webpages, blogs etc. but remains a possibility for archives providing access to recent PDArcs. See Lenthall, E. & Harman-Wilson, R. (2008) The Web of Contempt: A trap for website operators? *Computer Law & Security Report* 24(6): 568-570

41 Procter, M. (2006) 'The end of [local] history': will twenty-first century sources survive? *Local Historian* 36(4): 238-253

42 See the Personal Archives Accessible in Digital Media (paradigm) project http://www.paradigm.ac.uk/index.html

- draw up internal policies for processing incoming PDArc materials according to the risk assessment; for handling legal risks should they materialise; and for allocating responsibility for ensuing that internal policy is adequately disseminated to staff, and is followed;
- draw up appropriate deposit guidelines and advice on legal issues for would-be depositors of PDArc materials.

As discussed below (Section 4), archives and repositories may also have to consider adopting new strategies and processes to reduce the administrative overhead of legal compliance, and reduction of legal risk, in PDArcs, in order to be able to collect and provide access to a broader range of digital materials.

The following sections (2.1-2.4) provide an overview of the key legal issues that archives and repositories are likely to face, and an assessment of their effect on the collection and reuse of personal digital archives.

2.1 Copyright

Copyright is a property right vested in the owner of a protected work, and is essentially a bundle of economic and moral rights. In the UK the basic legal framework is contained in the *Copyright, Designs and Patents Act 1988* (CDPA 1988), as amended by later primary and secondary legislation.[43]

Copyright comes into being when a work is created, and no formal registration process is required, or available, in the UK. For a work to attract copyright protection the CDPA 1998 requires that it must be 'original'.[44] It need not be especially imaginative, but its creation must involve some effort and it cannot be just a copy of another work. [45]

Copyright only exists for a limited period - the term of copyright – and all works eventually emerge from copyright protection. Under UK law, different types of work have different terms of copyright protection.[46] Also, despite the harmonising role played by international agreements, different countries apply different terms of copyright protection to works. Thus, the basic term of copyright in the EU is author's life + 70 years, but in the UK the term of copyright for sound recordings is 50 years from the end of year in which they are made or published.

Copyright covers many types of creative effort. It protects specific classes of works, but not ideas. For example:

- *Literary Works*:[47] Popular understanding of literary works includes fiction and non-fiction books, journals and newspapers/magazines, but the category is much wider. The basic criteria are that the literary work is original and 'fixed' in some medium. This means that letters, e-mail messages, and webpages can all be the subject of copyright. A work's 'literary merit' is unimportant. The CDPA 1988 brought the spoken word within the scope of 'literary works', but requires spoken or sung words be 'recorded, in writing or otherwise ...' before a copyright can exist.[48]
- *Artistic Works*:[49] Includes graphic works, photographs, sculptures, collages, maps, charts and plans. These are protected regardless of artistic merit.

---

43 UK *Copyright, Designs and Patents Act 1988*: http://www.ipo.gov.uk/cdpact1988.pdf
For more detailed overviews, see Padfield, T. (2007) *Copyright for Records Managers and Archivists* (3rd ed.) Facet Publishing; Pedley, P. (2007) *Digital Copyright* (2nd ed.) Facet Publishing

44 s.1(a) CDPA 1988

45 *Ladbroke v William Hill* [1964] 1 WLR 273

46 s.12-15 CDPA 1988

47 s.3 CDPA 1988

48 Phillips, J. (1989). Copyright in Spoken Words - Some Potential Problems. *European Intellectual Property Review* (No.7) 231-234

49 s.4 CDPA 1988

- *Sound Recordings*:[50] Includes every type of sound recording on any type of medium from which sounds can be reproduced.
- *Films*:[51] this includes any medium from which a moving image may be reproduced.
- *Broadcasts*:[52] this includes any transmission capable of lawfully being received by members of the public.

Several copyrights may subsist simultaneously in a single item, such as a book or a webpage.

Ownership of copyright in a work can change hands after its initial creation, and like any property, can be bought, sold or inherited. It is important to remember that copyright in a work is separate from physical ownership of the work. Ownership of copyright in a work belongs, initially, to the person who created it.[53] This is subject to exceptions, which differ between countries, e.g. under UK law, copyright in works created in the course of employment does not vest in the employee, but in their employer, and thus the employer is the first owner.[54] This exception does not apply to contractors.

Copyright in the spoken word is slightly more complicated. For example, if a person is talking about a subject and the discussion is not recorded in any way, then there is no copyright in the spoken word – the talk has not been 'fixed'. However, if another person records that speech on a tape recorder, at that moment the work is 'fixed' and a copyright crystallises. In such circumstances, it appears that the speaker will have a copyright in their words, and the other person (technically, the 'producer' of the sound recording under the CDPA 1988) a copyright in the recording of those words. Thus, in order to use the recording, it will be necessary to secure permissions from both the speaker and the individual who 'produced' the recording. The same will be true of an audiovisual recording (technically, under the CDPA 1988, a 'film') of the talk, where both the speaker and some other person or persons (technically, under the CDPA 1988, the producer and the principal director) will own copyrights in the resulting recording.[55] If the speaker is reading from a written script or paper, there will be a copyright in the text, which is already 'fixed', and a joint copyright owned by the speaker and the individual who 'produced' the recording, in the recording.

A copyright owner has the right to prevent other people from, without permission:

- copying the work;
- issuing copies of the work to the public;
- performing or broadcasting the work;
- adapting, or amending the work.[56]

Copying is defined as reproducing the work in a material form, including storing the work in any medium.[57] If someone carries out these 'restricted acts' on a work without the owner's permission, or authorises someone else to do so, they are infringing the copyright in the work.

Where an individual collects material in which another person holds a copyright (e.g. a recording of a presentation in which the interviewee holds a copyright in their spoken words), and wants to use

---

50 s.5A CDPA 1988

51 s.5B CDPA 1988

52 s.6 CDPA 1988

53 s.11(1) CDPA 1988

54 s.11(2) CDPA 1988

55 It is worth noting that the CDPA 1988 does not appear to have caught up with the concept of 'user created content' or that individuals other than professionals will make sound recordings or 'films' ('film' means a recording on any medium from which a moving image may by any means be produced)

56 s.16 CDPA 1988

57 s.17 CDPA 1988

that material in another work, such as an article, a book, or event proceedings etc, they have a number of options. They could obtain an outright transfer of the copyright from the copyright holder (assignment - which must be in writing); they could obtain the copyright holder's permission do some of the things reserved to the copyright holder (licence - which need not be in writing),[58] or they could investigate whether any copyright exemptions or defences would cover their proposed use.[59]

The CDPA 1988 also introduced the concept of "moral rights" into UK legislation. These are distinct and separate from property rights and include:

- The right of the author of a work to be acknowledged as author or creator
- The right not to have their work subjected to 'derogatory' treatment
- The right of an individual to refuse to be associated with something they did not create.[60]

Moral rights cannot be transferred,[61] but can be waived.[62] Some do not apply to computer programs; works reporting current events; works that have appeared in newspapers, magazines, learned journals, or other collective works; actions required by law or by a Court, and to most employee created materials.[63] An individual might, for example, wish to be identified as the author of their spoken words, as recorded by an interviewer.

2.1.1 Application to Personal Digital Archives

Copyright risks may be assessed according to the likelihood of their occurrence, the likely consequences and the acceptability of their occurrence. Where risks are likely to occur, or their occurrence would have significant impact on a repository, then remedial measures will be required, including the development of clearly stated policy provisions. Much of the risk for a repository can be handled by developing a policy framework which provides for appropriate licensing mechanisms for deposited material and any other contributions, given the nature and scope of a particular repository, as well as processes to ameliorate the effect of any copyright infringements. However, the processes of licensing and risk management have to be balanced against the need to encourage individuals with PDArcs to engage with a repository. The key aim for repository owners should thus be to develop both licensing and risk amelioration processes which are as simple and transparent as possible to those wishing to deposit or access repository materials.

Handling IPR/copyright risks from the repository perspective

Repository owners will need to have a clear understanding of the copyright risks that their particular repository faces; this will require a careful risk assessment as early as possible in the developmental process. It is also essential that repository owners ensure that processes are in place to ensure that risk management is an ongoing issue, and that responsibility for undertaking such assessment, as well as developing and administrating methods of handling any risks identified, is clearly located within the staffing structure of the repository.

Current repository licensing trends

In terms of trends in existing practice in addressing copyright issues, there is a degree of support among stakeholders in all types of digital repositories for the adoption of clear and concise copyright licensing options like those provided by the Creative Commons (CC) project. What is also clear, however, is that:

---

58 s.90 CDPA 1988

59 s.28-76 CDPA 1988

60 s.77, s.80, s.84 CDPA 1988

61 s.94 CDPA 1988

62 s.87 CDPA 1988

63 s.79, s.81 CDPA 1988

- using CC licences still requires at least a basic understanding, on behalf of both licensor depositors and licensee users, of how copyright licensing works, and what is being granted (or not) by the licensor, and such knowledge is by no means universal;
- it is often the case that IP rights in PDArcs may be vested in third parties other than the depositor; for the repository to make use of those resources may thus require the depositor to seek additional permissions;
- the licence options available under the CC do not necessarily provide a complete solution to a repository's needs, e.g. if some depositors want more specific/restrictive terms;
- even if CC licences (or variants thereof) are used, there remains the issue of how to deal with the results of the unintended or unsuspected incorporation of unlicensed third party material within PDArcs.

As such, CC licences are not a panacea for all deposit and access-related copyright issues arising in repositories.[64] Depending on local or sectoral factors, repositories seeking to accession PDArcs may be better served by variants based on CC licences or, indeed, entirely different licensing models. Early assessment of those factors will play a key role in aiding repository owners in choosing an appropriate licensing mechanism.

Simple copyright licensing processes for deposit

Obtaining a viable set of quality digital objects through PDArc deposit is a vital objective for any repository. It is important, therefore, that processes designed to facilitate copyright compliance, and to ameliorate risk, do not have the undesired consequence of deterring potential depositors. The nature of the digital objects to be deposited will influence the willingness of would-be depositors to engage with repository processes. It will be important for repository owners to assess the likely factors that will affect willingness to deposit, and to tailor their processes accordingly, for example:

- a requirement on depositors to create rights metadata for deposited materials would until recently have been seen as a negative factor in encouraging deposit; however, increasing use of Web 2.0 technologies, such as 'tag clouds', may mean that PDArc creators/depositors are more willing to accept the benefits of metadata usage, and thus some additional overhead to deposit processes;
- providing a small set of licence choices from which depositors can choose will reduce confusion, but may also restrict the number of depositors who are able or willing to contribute under the sets of licence terms available to them.

Part of this process will involve identifying areas in which a repository can enhance understanding through provision of a tailored range of information on licensing, and outreach mechanisms such as guidance and guidelines on IPR for depositors.

Simple copyright licensing processes for access

'If we build it, they will come' often appears to be an underlying conviction for those planning repositories for digital objects. However, simply providing access to digital objects is unlikely to result in significant uptake and use where potential users are uncertain about the consequences of using such material. Just as with depositors, it is important that processes designed to facilitate copyright compliance, and ameliorate risk, do not have the undesired consequence of deterring access and reuse. Repository owners will need an understanding of the factors that are likely to attract or deter would-be users of differing types of PDArc, and to have a strategy for addressing those factors, for example:

- Most of those seeking to use digital objects contained in PDArcs are unlikely to want to have to spend significant amounts of time working out what they can and can't do under the licence applicable to those objects. Use of quick mechanisms for identifying acceptable

---

64 Korn, N., Oppenheim, C. (2006). Creative Commons licences in higher and further education: Do we care? *Ariadne*, 49 http://www.ariadne.ac.uk/issue49/korn-oppenheim/

licences, such as icons representing key licence conditions, will help to reduce both confusion and time overheads.

Here, too, a repository can increase its accessibility and value to would-be users by providing a tailored range of information on licensing conditions ranging from short explanations to full licence agreements.

Future-proofing

The role of most digital object repositories is unlikely to be a static one. Even as new repositories are being created, their owners (or their users) are often seeking new ways to add value to their content and/or services. As the functions of repositories become more diverse (e.g., by seeking to incorporate both non-commercial and commercial digital content, or by incorporating third party input about digital objects, such as commentary or reviews), their owners' strategies for handling the resulting copyright issues will inevitably become more complex. As a result, it is likely to be necessary for would-be repository owners to be planning and implementing a medium to long-term copyright strategy even before the repository is established. The range of approaches to copyright and licensing adopted by existing digital resource repositories in other areas (such as digital learning archives) in support of particular business models, highlights the importance of addressing the copyright issues of a repository owner's desired or potential business model at an early stage.

2.1.2 Information gathering and risk assessments (deposit and access)

The repositories that handle the copyright/IPR issues arising from their activities most effectively are those which scope the issues pertaining to their planned repository well in advance of launch. This allows them sufficient time to:

- access and learn from relevant experience derived from existing repositories and from other related projects;
- identify particular issues relevant to:
  - the nature of their repository
  - the specific type of materials they intend to accept
  - the particular type(s) of PDArc depositor and accessor they intend to serve
  - the intellectual property regime of their jurisdiction
  - the prevailing political and social circumstances;
- assess key issues of concern to depositors and accessors and to develop strategies to reduce the impact of those concerns on the use of the repository.

Repositories that have undertaken a considered review of their operating environment are better placed to apply an appropriate and efficient level of risk management. Whilst a risk management process cannot guarantee a successful copyright/IPR strategy immediately (even those repositories that have spent considerable time on backgrounding and risk assessment may find that their initial solutions are incomplete or over-cautious), it does provide a basis from which later copyright/IPR policy changes for both deposit and access can be adopted in a structured and coherent fashion.

2.1.3 Choice of licence regime (deposit and access)

The choice of licence regime is highly likely to be influenced by the outcomes of the backgrounding and risk management processes. There are essentially four decisions to make with regard to the licensing regime:

- For deposits:
  - Is the repository going to target 'high profile' contributions, or 'digital public' contributions, or any offered PDArcs?
- For access:
  - What kind of access conditions, if any, is the repository prepared to/able to accept with regard to any offered PDArcs?
- For both:

- Is the repository going to act as a licensor (by taking an assignment of copyright from the depositor and licensing to users), licensee (by taking a licence of copyright from the depositor, and sub-licensing to users) or unlicensed intermediary (by providing the mechanism through which users can obtain a licence of copyright from the depositor)?
- Are the licences to be used going to be unmodified Creative Commons licences, bespoke licences (i.e., licences based on terms specific to the repository), or a combination of the two (e.g., a Creative Common style licence with additional clauses)?

It is clear that the choices made will affect the complexity of the licensing process, the likelihood of depositors making materials available and the willingness of users to access and use the materials. There is a balance to be struck between a regime that meets the interests of depositors, facilitates the goals of the repository and encourages access to any reuse of digital objects within PDArcs. It is probable that there is not going to be one optimal approach to reaching this balance, not least because those three factors are likely to differ between repositories.

2.1.4 Confusion over copyright ownership (deposit)

There remains a great deal of confusion over who owns copyright in particular types of work, for example, letters, e-mails and other forms of personal correspondence. This confusion largely derives from a widespread lack of:

- coherent and concise guidance on, and explanation of, the basic rules of copyright, i.e., that in the UK an individual who creates an original work will own the copyright in that work UNLESS:
  - the work is created in the course of their employment (noting that where, when, and on whose equipment, the work is made is usually irrelevant to the determination of what is entailed by 'in the course of their employment'), when it will belong to their employer, unless otherwise agreed;
  - there is a contractual agreement that the rights in the work will belong to a third party; or
  - there is legislative or other legal provision that the rights in the work will belong to a third party.
- clear legal and ethical guidelines on the acceptable ways of using/reusing materials that have been created by third parties, such that creators of original digital objects receive appropriate recognition.

Where there is poor understanding of the law, and particularly where there are no accepted cultural/administrative methods of reinforcing moral and ethical standards, levels of trust decline, and individuals are more likely to resort to asserting legal claims (their 'rights') or simply withholding materials, both of which reduce the likelihood of deposit with repositories and make reuse of materials less likely.[65]

2.1.5 Confusion over licence terms (deposit and access)

While a repository may choose a particular licensing regime, including the use of a particular licence or set of licences, the issue remains that many depositors and users remain unaware of, or confused about, the implications of the terms of those licences. This may lead to depositors:

- choosing a licence which places more restrictions on the use of their material than they intended
- accidentally permitting uses of their material (such as commercial use) that they did not intend

---

[65] Charlesworth, A. Ferguson, N. Massart, D. Van Assche, F. Mason J. Radford, A. Smith, N. Tice, R. Collett, M. Schmoller, S. (2008) *Development of Good Practice Guidelines for Repository Owners*, Project Report, BECTA, 14 February 2008

- not depositing material because they do not want to take the time to work out what the licence or licences permit
- depositing unsuitable material (e.g., material in which a third party holds rights, and which has not been appropriately licensed for deposit).

Equally users may:

- use material for purposes for which they are not licensed
- not use material because they think the licence is more restrictive than in fact it is
- not use material because they can't decide what is, and is not, being licensed.

Making the licence choice, for both depositors and users, as simple as possible in the circumstances is thus an important aim for repository owners. Techniques for achieving this include:

- adopting a single licence for all deposits (this has the benefit of simplicity, but the downside of all 'one-size-fits-all' approaches – one size usually doesn't fit all);
- adopting multiple licences, but providing a range of materials explaining in varying levels of detail what the licences mean (this provides more options for depositors, but places more overhead on the deposit process, and may confuse or deter users);
- using icons to identify the key licence terms applicable to particular materials. This has the advantage of brevity and simplicity, but requires a licensing system whose terms can be broken down into icon form, and, ideally, different repositories should use the same or a similar range of icons to indicate the same terms – this is not uniformly reflected in current practice in digital repositories;
- ensuring that depositors are encouraged (or mandated) to complete ownership and licensing metadata within the repository's metadata records when depositing material (views are mixed as to whether this will be a significant deterrent to potential depositors – there is a growing belief that it will not, as use of metadata elsewhere becomes more common).

2.1.6 Risk management processes (organisational)

A key issue in establishing an effective copyright/IPR policy framework is that of ensuring appropriate organisational management of copyright risk. Dealing consistently and effectively with the copyright/IPR issues raised by a repository, both at start-up and during operation, will require the clear allocation of responsibility for those determining and addressing those issues within the repository's management team. That responsibility will span both the deposit and access functions of the repository, as changes to the copyright/IPR policy on the one side will almost inevitably have repercussions on the other. Effective copyright/IPR risk management is vital to establishing and maintaining both depositor and user trust in the reliability of a repository.

2.1.7 Policy framework/holistic approach (organisational)

It is important when developing policy in this area to take a holistic view of the copyright/IPR issues. Building a flexible copyright/IPR policy framework, based on the initial background and risk assessment, which contains clear and documented processes for deposit and access management, policy and process audit and risk amelioration, and which incorporates the ability to effect coherent change management in the light of shifts in environmental factors, will be essential to long-term sustainability.

2.2 Data Protection and Privacy

The *Data Protection Act 1998* (DPA 1998)[66] provides individuals with certain rights regarding information held about them. It places obligations on those who are responsible for processing personal data (data controllers) and gives rights to those who are the subject of that data (data

---

66 Data Protection Act 1998 http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

For more detailed overviews, see Jay, R. & Hamilton, A. (2007) *Data Protection Law and Practice* (3rd ed.) Sweet & Maxwell; Carey, P. (2009). *Data Protection: A Practical Guide to UK and EU Law*. (3rd ed.), Oxford University Press

subjects).[67] Processing of personal data for research purposes falls under the general provisions of the Act, but some specific research-related exemptions are provided.

The DPA 1998 addresses the lawful processing of personal data. It defines personal data as any information relating to an identified/identifiable living person, or which in combination with other information held by or available to the data controller, would permit their identification.[68] Fully anonymised data is outside the Act, but pseudonymised or coded data is covered, as a pseudonym or code can be linked back to an identifiable individual. Additionally, for the Act to apply, the personal data must be, or intended to be, processed by computer or other equipment, or included in certain types of structured manual records.[69]

Some types of personal data are given greater protection. These are labelled as sensitive personal data. Personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences fall under this heading.[70]

Data processing is defined in the Act as 'obtaining, recording or holding the data or carrying out any operation or set of operations on the data.' This includes collection, recording, organization, storage, adaptation/alteration, retrieval, consultation, use, disclosure by transmission/ dissemination, alignment/combination, blocking, erasure or destruction.[71] The breadth of the definition essentially means that from its collection, to its destruction or full anonymisation, personal data is being 'processed' and thus the Act applies.

The DPA 1998 places a set of obligations upon data controllers: failure to observe these obligations will breach the Act and can result in legal sanctions, including fines and prohibitions on processing.[72] While large fines are rare, such breaches may bring significant bad publicity. From the point of view of individuals and institutions working with personal data, publicised breaches may result in other negative consequences e.g. disciplinary action by employers, future difficulty in obtaining research and development funding, and unwillingness of potential data subjects to engage with institutional projects.

For all personal data, at least one of the following conditions must be met for personal information to be 'fairly processed':

- the individual has consented to the processing

or that the processing is:

- necessary for the performance of a contract with the individual
- required under a legal obligation (non-contractual)
- necessary to protect the individual's vital interests
- necessary to carry out public functions, e.g. administration of justice
- necessary in order to pursue the data controller's or a third party's legitimate interests and not unfair to the individual.[73]

Under UK data protection law, consent is thus not an absolute requirement for processing; a data controller may process non-sensitive personal data under another condition. However, data

---

67 s. 1(1) DPA 1998

68 s. 1(1) DPA 1998

69 s. 1(1) DPA 1998

70 s.2 DPA 1998

71 s.1(1) DPA 1998

72 s. 60 DPA 1998

73 Schedule 2 DPA 1998

controllers must still provide information to data subjects about the purpose of the processing, and possible third party recipients of the personal data.

The processing of sensitive personal data is subject to more stringent conditions. The conditions for processing sensitive data are that one of the above conditions has been met AND the data subject has given her explicit consent to the processing, OR that the processing is necessary for a further set of specified reasons, including that it is:

- required by law for employment purposes
- needed to protect the individual's, or another person's, vital interests
- needed in connection with the administration of justice or legal proceedings[74]

The meanings of "consent" and "explicit consent" are not defined, although the latter is often perceived as meaning "in writing" (it need not be). If no consent is forthcoming and the purpose of particular processing is not otherwise on the list of permissible reasons, it will be unlawful.

All personal data processing, unless exempted, must conform to 8 Data Protection Principles.[75] These require that data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the individual's rights
7. kept securely
8. not transferred to countries outside European Economic Area unless the country in question has adequate protection for individual privacy.

There are specific exemptions from some of the Principles for personal data processed for research purposes.

The Act gives rights to individuals over their personal data held by data controllers.[76] Failure to respect these rights may result in civil or criminal actions. Most data subject rights are linked to, and/or depend for their usefulness upon, the availability of an effective right of subject access. Subject access means that a data subject is entitled to be told by a data controller whether personal data about them is being processed by, or on behalf of, that data controller, and to be given access to a copy of that data. The rights include the ability to:

- make subject access requests
- prevent processing likely to cause damage or distress
- prevent processing for direct marketing purposes
- take action for compensation if they suffer damage caused by breach of the Act
- take action to rectify, block, erase or destroy inaccurate data,
- request the Information Commissioner to assess whether the Act has been breached

As with the Data Protection Principles, there are specific exemptions from data subjects' rights for personal data processed for research purposes.

The DPA 1998 provides exemptions for 'research purposes' including statistical or historical purposes.[77] Where processing for research purposes is not used to support measures or decisions targeted at particular individuals, and will not cause substantial distress or damage to a data subject, it is exempt from:

---

74 Schedule 3 DPA 1998

75 s.4 & Schedule 1 DPA 1998

76 s.7-15 DPA 1998

77 s.33 DPA 1998

- The Second Principle - *personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes* - personal data can be processed for research purposes other than for which they were originally obtained
- The Fifth Principle - *personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes* - personal data processed for research purposes can effectively be held indefinitely

Additionally, where:

- personal data is not processed to support measures or decisions with respect to particular individuals;
- personal data is not processed in a way that substantial damage or distress is likely to be caused to any individual;
- the research results, or any resulting statistics, are effectively anonymised;

there is an exemption from the data subject's right of access. The data controller may still choose to disclose the information to the data subject, unless by doing so they would breach another individual's data protection rights.

In addition to the legitimate purposes for processing of sensitive personal data contained in the DPA 1998 (e.g. explicit consent, medical research by a health professional), the *Data Protection (Processing of Sensitive Personal Data) Order 2000*[78] expressly permits processing for research purposes 'in the substantial public interest' where the data are not used to support measures or decisions targeted at particular individuals without their explicit consent; and no substantial damage or distress is caused, or is likely to be caused, to any person by the keeping of those data.

While some exemptions are granted for use of personal data for research purposes; there is no blanket exemption from the Data Protection Principles. Thus:

- Research data subjects should be informed of any new data processing purposes, the identity of the data controller, and any disclosures that may be made.
- Research data subjects must be able to meaningfully exercise their right to object to the data processing because it would cause/has caused, them significant damage or distress.
- Requirements for appropriate security of data must be respected, including appropriate levels of security for sensitive data
- Data may not be transferred to researchers in a non-EEA country, unless that country provides adequate data privacy protections, the data subject's explicit consent has been obtained, or there is an appropriate data protection contract with the data recipient.

The legislation recognises that the value of access to personal data in research may outweigh a data subject's desire to exercise a high level of control over the use of their data. As a result, even researchers wishing to use sensitive personal data should be able to do so, if they can demonstrate a significant public interest, and they adhere to the procedural safeguards required by law.

2.2.1 Application to Personal Digital Archives

Data protection risks may be assessed according to the likelihood of their occurrence, the likely consequences and the acceptability of their occurrence. Where risks are likely to occur, or their occurrence would have significant impact on a repository, then remedial measures will be required, including the development of clearly stated policy provisions. A significant issue for repositories will be the fact that most of the information contained in PDArcs will have been collected by individuals in the course of their personal, family or household affairs. This material is, while it is used for those purposes, specifically exempted from the DPA 1998.

> s.36 Domestic purposes - Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt

[78] The Data Protection (Processing of Sensitive Personal Data) Order 2000, s.9 http://www.opsi.gov.uk/si/si2000/20000417.htm

> from the data protection principles and the provisions of Parts II [rights of data subjects] and III [notification of processing].

However, once this material is deposited with a repository, that exemption will end, and the Act will apply to further uses of any personal data contained in the PDArc, except insofar as they are exempted by other provisions, such as the research, history and statistics exemption (s.33 DPA 1998), or the research exemption in the *Data Protection (Processing of Sensitive Personal Data) Order 2000*. The repository will thus need to be aware of its obligations under the Act, and the criteria that need to be met in order to retain the protection of the research exemptions.

Repositories may find that digital material carries a longer term DP obligation than analogue material:

> If digital archives are accessioned earlier than paper archives have been in the past, then archives could potentially be subject to the provisions of the Data Protection Act for much longer while they are being managed by an archival repository. … Repositories may therefore find themselves managing a significant number of collections which are closed to researchers and could come under pressure from historians of the contemporary period to release items. The processes involved in acquisition, appraisal and cataloguing should identify data protection issues so that they can be managed appropriately.[79]

As with copyright, a repository will need to develop an appropriate policy framework for handling data protection issues arising out of deposited material which is as simple and transparent as possible both to those wishing to deposit or access repository materials, and to those whose personal data is, or maybe, included in a PDArc.

Handling data protection risks from the repository perspective

Repository owners will need to have a clear understanding of the data protection risks that their particular repository faces; this will require a careful risk assessment as early as possible in the developmental process. It is also essential that repository owners ensure that processes are in place to ensure that risk management is an ongoing issue, and that responsibility for undertaking such assessment, as well as developing and administrating methods of handling any risks identified, is clearly located within the staffing structure of the repository.[80]

Current repository trends in data protection handling

The literature addressing data protection issues in archived digital materials is considerably thinner than that available for copyright. As such, it is harder to identify clear trends in existing practices amongst repositories. Where material is available, archives appear to apply the same rules to material covered by the DPA 1998, whether it is in analogue or digital format. For example, the National Archives' policy on data protection does not differentiate between them:

> **4 Data protection and our archival holdings**
>
> 4.1 The Data Protection Act applies to all archives that contain personal information about identifiable living individuals. …
>
> 4.2 Where personal information in archives is being processed solely for the purposes of archival preservation, and is not accessible to the public, we can claim exemption from most of the Data Protection Principles and from the obligation to respond to access requests from data subjects.

---

79 The Personal Archives Accessible in Digital Media (paradigm) Project: Data Protection http://www.paradigm.ac.uk/workbook/legal-issues/dpa.html

80 Some guidance on these issues in the UK is provided by the National Archives, although this guidance is general in nature and does not explicitly deal with issues arising from PDArcs. See National Archives (2000) *Data Protection Act 1998:A Guide for Records Managers and Archivists*, Public Record Office http://www.nationalarchives.gov.uk/documents/dpguide.pdf

National Archives, Society of Archivists, Records Management Society & National Association for Information Management (2007) *Code of practice for archivists and records managers under Section 51 (4) of the Data Protection Act 1998*, The National Archives http://www.nationalarchives.gov.uk/documents/dp-code-of-practice.pdf

> However, as a matter of policy, we will respond to access requests when an individual's rights or entitlements seem to be at stake, in recognition of our role as a public body.[81]

This is then reiterated in the National Archives' procedures document:

> **12 SUBJECT RIGHTS TO PERSONAL DATA IN THE ARCHIVES**
>
> …
>
> 12.1 The Data Protection Act applies in general to archives containing personal information about identifiable living individuals, both electronic archives and those in traditional formats such as files, bound volumes or indexes.
>
> 12.2 Data subject access rights apply to archives covered by the Act but we will claim an exemption if the archives are closed to the public, under section 33(4) of the Act, on the grounds that
>
> - the records are being processed in a way that does not reveal the names of data subjects; and
> - this processing does not cause those data subjects substantial damage or distress; and
> - the processing does not involve decision-making affecting the data subjects
>
> 12.3 However, even when the exemption can be claimed, as a matter of policy we will respond when the applicant has a real need of the information in recognition of the fact that we are a public institution that should, where possible, provide information necessary for tax payers to claim their rights and entitlements. … [82]

A working rule for whether materials are likely to contain information about living individuals can be found in the National Archives' Code of Practice:[83]

> 4.1.5 Given the large number of individuals commonly featuring in archive collections, archivists will not be in a position to ascertain whether they are still alive and hence protected by the Act. If it is not known whether a data subject is alive or dead, the following working assumptions can be used:
>
> - Assume a lifespan of 100 years
> - If the age of an adult data subject is not known, assume that he was 16 at the time of the records
> - If the age of a child data subject is not known, assume he was less than 1 at the time of the records

As noted above, if digital materials are deposited at an earlier stage than paper records, i.e. a collector decides to deposit a PDArc while they are still alive, because they are able to retain an electronic copy of the materials that they have deposited, there may be pressure on archives in the future to release prior to the 100 year 'rule'. Equally, as users become used to easy access to the personal information of others with little delay, e.g. through social networking services, and social norms about what kinds of data would normally be kept private change, the appropriateness of this 'rule' may be called into question.

Simple data protection processes for deposit

The National Archives' Code of Practice states that:

> 4.4 Accessioning
>
> 4.4.1 All newly received archives, whether manual or electronic, should be checked to ascertain whether they include personal data covered by the Act …

---

81 National Archives (2008) Data Protection Policy Statement http://www.nationalarchives.gov.uk/legal/pdf/policy-feb08.pdf

82 National Archives (2008) Procedures for handling personal information under the Data Protection Act 1998 http://www.nationalarchives.gov.uk/legal/pdf/procedures-feb08.pdf

83 Above, n.80

While such checking may be feasible for pre-arranged deposit of limited numbers of 'high profile' PDArcs, such a process is going to be problematic in circumstances where a repository wishes to accession large numbers of 'digital public' PDArcs. Digital material may, however lend itself to other forms of less time intensive prior checking, including automated data mining techniques, depositor-generated metadata and depositor tagging.

Simple data protection processes for access

The National Archives' Code of Practice states that:

> 4.1.6 When researchers obtain copies of personal data from an archives repository they become the data controllers in respect of those copies and must observe the data protection principles, unless they can claim an exemption, for example because their processing is for domestic purposes only, i.e. personal, family or household use. However, archivists cannot control subsequent use of personal data and it is advisable to assume that researchers will be subject to the Act and make them aware of their responsibilities.

The Code of Practice appears to be premised upon there being a clear distinction between 'users' and 'researchers'. The former may be excluded from access to archived materials containing personal data for up to 100 years, the latter will be able to take advantage of the research exemptions in the DPA 1998 and secondary legislation, and gain access at an earlier date.

It is suggested here that this 'rule' is an artefact of the social environment in which the DPA 1998 was drafted, when the type of data envisaged as being placed in archives was primarily government or corporate data, with some 'high profile' personal data collections. The 'rule' may be less suited to a social environment where PDArcs and particularly 'digital public' PDArcs are being sought for accession and reuse. However, solutions to that issue are likely to lie with legislative reform of the DPA 1998, rather than with the policies and practices of archives and repositories.

At present, repositories will need to consider how they control both access to, and potential reuses of, digital materials from PDArcs. As the Code of Practice suggests, providing effective guidance to researchers as to their obligations and responsibilities will be a key part of that process. As with copyright, it is important that:

- processes designed to facilitate data protection compliance, and ameliorate risk, do not have the undesired consequence of deterring legitimate access and reuse;
- legitimate researchers are able to determine the rules applicable to the use and reuse of the personal data they are accessing

Future-proofing

As with copyright, data protection law is a developing area. This is not least because the Data Protection Act 1998 is coming under increasing criticism as being technologically and socially outdated,[84] as well as ineffective at achieving its goal of protecting the rights of data subjects in a context-sensitive fashion.[85] Repositories should thus be thinking carefully about how they structure their deposit conditions and access mechanisms for accessioned PDArcs to ensure that they do not inadvertently lock digital information into an inflexible data access and reuse framework that cannot readily respond to a changing data protection environment.

2.2.2 Information gathering and risk assessments (deposit and access)

The repositories that handle the data protection issues arising from their activities most effectively are those which scope the issues pertaining to those activities well in advance of beginning the accession process. This allows them sufficient time to:

- identify current best practice guidelines, e.g. the National Archives' Code of Practice;

---

84 Charlesworth, A. (2006). The future of UK data protection regulation. *Information Security Technical Report* 11(1): 46-54

85 Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review* 79(1): 119-158

- access and learn from relevant experience derived from existing repositories and projects, e.g. the National Archives' Procedures for handling personal information, or the Digital Curation Centre's Briefing paper on data protection;[86]
- identify particular issues relevant to:
    - the nature of their repository
    - the specific type of materials they intend to accept
    - the particular type(s) of PDArc depositor and accessor they intend to serve
    - the data protection regime
    - the prevailing political and social circumstances;
- assess key issues of concern to depositors and accessors and to develop strategies to reduce the impact of those concerns on the use of the repository.

Repositories that have undertaken a considered review of their operating environment are better placed to apply an appropriate and efficient level of risk management. Whilst a risk management process cannot guarantee a successful data protection strategy immediately (even those repositories that have spent considerable time on backgrounding and risk assessment may find that their initial solutions are incomplete or over-cautious), it does provide a basis from which later policy changes for both deposit and access can be adopted in a structured and coherent fashion.

2.2.3 Data protection roles and responsibilities (deposit and access)

As already noted, when an individual deposits their PDArc with a repository, this will trigger certain responsibilities on behalf of the repository, which were not applicable to the individual when they were using the digital materials for their personal, family or household affairs. It is thus important to the future use of the PDArc that the repository has a clear understanding of what information it requires in order to effectively accession it. This may mean obtaining a clear picture of what, if any personal data they are receiving, at the time of transfer, and ensuring that the depositor understands the importance of providing the repository with information relevant to the data privacy status of the materials deposited. Where the repository's risk assessment for the type of data to be accessioned suggests it is necessary, the depositor might also be asked to warrant that the information they have provided about the status of any personal data is accurate.

In liability terms, providing access to material containing personal data in breach of provisions of the DPA 1998 will have the potential to be more damaging to a repository, both legally and reputationally, than accessioning such material. Presently, for personal data for which no consent has been obtained from the data subject for making it available to third parties, there are limited grounds under which it can be fairly and lawfully made available. For non-sensitive personal data, recourse may be had to other conditions in Schedule 2 DPA 1998 (e.g. that the access is necessary in order to pursue a third party's legitimate interests and is not unfair to the individual), or other exemptions in the Act (e.g. the research exemption). For sensitive personal data the available options are considerably more restricted (e.g. the research exemption in secondary legislation). Additionally, a data subject may have notified the repository that they consider access to their personal data held in a PDArc may cause them damage or distress. While this is not an outright bar to access, the repository must consider whether, in the circumstances, it is justifiable to provide access to the data in question.

It appears therefore that it will be necessary to have more restrictive oversight of access to personal data in PDArcs than of deposit. This means that access will require more stringent processes and safeguards in place. The National Archives' Code of Practice suggests that repositories should take the following measures to ensure as far as possible that third parties process any personal data lawfully:

> Steps to safeguard the fair and lawful use of data include:

---

[86] Digital Curation Centre (2007) Briefing Paper: Data Protection http://www.dcc.ac.uk/resource/briefing-papers/data-protection.pdf

- Explaining to intending researchers the "relevant conditions" that apply to the research use of particular data, including sensitive personal data.
- Requiring researchers to sign a declaration that, as a condition of access to data that might otherwise be closed, they will comply with the relevant conditions and Data Protection Principles (1, 3-4 and 6-8). Application forms to consult specific personal data subject to these conditions should be signed and kept as an audit trail.
- Informing researchers that they are responsible under the Act for any processing by them of personal data disclosed to them, including copying, realignment, transmission abroad and publication.
- If researchers are bound by a sectoral code of practice or particular employer requirements, e.g. guidelines produced by a university ethics committee, making access conditional on the researcher undertaking to comply with that as well as with any special conditions applying to specific sets of personal data. This is particularly relevant if he intends to publish or to make.

2.3 Freedom of Information

The Freedom of Information Act 2000 (FOIA) gives a general right of public access to all types of 'recorded' information held by public authorities, sets out exemptions from that general right, and places a number of obligations on public authorities. The Act only applies to 'public authorities' and not to private entities. However, public authorities are broadly defined in the Act, and include Government departments, local authorities, and a long list of other public bodies.[87] The Freedom of Information Act 2000 applies to England, Wales and Northern Ireland. A separate Act, the Freedom of Information (Scotland) Act 2002, applies to Scotland. Unlike the DPA 1998, the FOIA 2000 does not specify the way in which records are held. The Act covers all information "held" regardless of the form in which it is recorded. The fact that information is held digitally is irrelevant.[88]

Public authorities have two main responsibilities under the Act, production of a Publication Scheme[89] and handling individual requests for information.[90] A Publication Scheme is essentially a guide to the information the public authority holds which is publicly available. It must set out:

- the classes of information the public authority makes publicly available
- the manner in which the information is published, and
- details of any charges to access the information.

When deciding what information should be included in its scheme, a public authority must have regard to the public interest when:

- considering the degree of access to information provided;
- publishing the reasons for its decisions with regard to access.

Information included in the publication scheme is exempt from requests for information.

The Act also permits individuals to make a request to a public authority for information. The individual does not have to be the subject of that information, or be affected by its holding or use. Applicants are entitled to be informed whether the information is held by the public authority, and if it is, to receive a copy of the information, where possible in the manner requested, e.g. as a copy or summary, or in paper or electronic format. An individual may also request to inspect records in person.

---

87 s.3 & Schedule 5 *Freedom of Information Act 2000*

88 Digital Curation Centre (2005) Briefing Paper: Freedom of Information (McGinley, M.) http://www.dcc.ac.uk/resource/briefing-papers/freedom-of-information/

89 s.19 FOIA 2000

90 s.1 FOIA 2000

While the Act creates a general right of access to information held by public authorities, it also sets out 23 exemptions where that right is either disapplied or qualified.[91] There are two general categories of exemption: those where, even though an exemption exists, a public authority has a duty to consider whether disclosure is required in the public interest; and those where there is no duty to consider the public interest. The public interest test requires a public authority to consider whether the public interest in withholding the exempt information outweighs the public interest in releasing it. It involves considering the circumstances of each particular case and the exemption that covers the information. The balance is meant to lie in favour of disclosure, in that information may only be withheld if the public interest in withholding it is greater than the public interest in releasing it.

Exemptions where the public interest test applies, and which are most likely to apply to PDArcs are:

- personal information[92]
- legal professional privilege
- commercial interests

Where an institution considers that the public interest in withholding the information requested outweighs the public interest in releasing it, the institution must inform the applicant of its reasons, unless providing the reasoning would effectively mean releasing the exempt information.

These are then exemptions where, if the exemption applies, it is not necessary to go on to consider disclosure in the public interest. These include:

- information accessible to applicant by other means
- personal information[93]
- information provided in confidence
- disclosure is prohibited by an enactment or would constitute contempt of court.

A repository which qualifies as a public authority which wishes to rely upon a specific exemption must therefore ask itself a series of questions:

- Is the information potentially covered by an exemption?
- Does the exemption apply to all or part of the information requested?
- If an exemption does apply, does it require consideration of whether disclosure should be made in the public interest, irrespective of the exemption?
- If an exemption does apply, does it require consideration of whether disclosure would be prejudicial to a particular activity or interest?

Only the information to which an exemption applies can be withheld, e.g. if a particular document or file is requested which contains some exempt information, only those specific pieces of exempt information can be withheld. The rest of the document or file has to be released. If information is withheld under an exemption, the public authority must give reasons for its decision and inform the

---

91 s.21-44 FOIA 2000

92 Where disclosure would not breach any of the Data Protection Principles, but the individual who is the subject of the information has served notice under s.10 DPA 1998 that disclosure would cause unwarranted substantial damage or distress, or the individual who is the subject of the information would not have a right to know about it or a right of access to it under the DPA 1998, there is no absolute exemption and the public authority should consider the public interest in deciding whether to release the information

93 There is an absolute exemption if an applicant making a request for information under the FOIA is the subject of the information requested and they already have the right of 'subject access' under the Data Protection Act 1998; or if the information requested under the FOIA concerns a third party and disclosure by the institution would breach one of the Data Protection Principles

applicant of his right to complain to the Information Commissioner. Where an exemption applies, an institution may be required to release the information, by the Information Commissioner, in the public interest.

The Act provides for two Codes of Practice to be issued by the Lord Chancellor. The first Code concerns procedures for giving access to information.[94] The second Code sets out good practice in records management.[95]

2.3.1 Application to Personal Digital Archives

Not all repositories collecting PDArcs will be classed as 'public authorities' under the FOIA 2000, and those private repositories will remain largely unaffected by the legislation - although issues will clearly arise should private repositories transfer PDArcs from their collection to that of a repository that is classed as a public authority, such as the British Library,[96] or a repository attached to a University.[97] For repositories that are classed as public authorities, the obligations of the FOIA 200 will apply. However, this does not mean that all information that is held in a public authority repository will necessarily be subject to disclosure under the Act. According to the Information Commissioner's Office,

> As the Act relates to information that is "held by a public authority", … the definition may extend to information loaned or donated from third parties who are not public authorities.
>
> …
>
> Although the Act does not cover privately held information, there will be many cases when privately owned information is held by a public authority for its own purposes. … For example, an individual may donate his family archives to a library in order for them to be viewed by the public, either immediately or at some date in the future.
>
> In these circumstances the public authority will have an interest in this information and will make disclosure decisions. This is because although ownership may still rest with the depositor, the public authority with whom the information has been deposited effectively controls the information and holds it in its own right. It will therefore be difficult to argue that the information is merely held on behalf of another person and consequently not held for the purposes of the public authority itself.
>
> …
>
> There is a possible further category of information, namely information being deposited subject to conditions. In such cases it will often be considered incorrect to disclose information if there was a clear risk that the owner would demand its return or if the depositor had a reasonable expectation that disclosure would not take place. In these circumstances, the public authority which receives the request should check with the depositor, or surviving relatives, who will be able to advise the authority as to their wishes and expectations. Where the depositor of the information objects to its disclosure, it will usually be found that an exemption can be applied to it. Exemptions which could apply are:
>
> - Information available by other means;
> - Personal Information;
> - Information provided in confidence;
> - Prejudice to commercial interests;

---

94 s.45 FOIA 2000 - *Lord Chancellor's Code Of Practice on the discharge of public authorities functions under Part I of the Freedom of Information Act 2000* (2004) http://www.justice.gov.uk/guidance/docs/foi-section45-code-of-practice.pdf

95 s.46 FOIA 2000 - *Lord Chancellor's Code of Practice on the Management of Records* (2002) http://www.foi.gov.uk/codemanrec.pdf

96 Schedule 1, Part VI FOIA 2000

97 Schedule 1, Part IV, s.53(1) FOIA 2000

- Prejudice to effective conduct of public affairs.[98]

This suggests that where PDArcs are deposited with a public authority repository, there can still be restriction placed on the use of material contained within it.

Two key exemptions stand out – the personal information exemption, and the confidentiality exemption. The former will allow an individual whose personal data is contained in the PDArc to seek to block disclosure, where that disclosure would cause them unwarranted substantial damage or distress – at that point the repository would have to make a reasoned determination as to whether the likelihood of that substantial damage or distress outweighs the public interest in disclosure.

In the latter case, if the information was provided to the repository 'in confidence' until certain conditions were met, that information may be exempted from FOIA entirely. An actionable breach of confidence is likely to exist where a party has breached a contractual obligation of confidence. However, it can also exist when there is no express contractual obligation of confidence provided the disclosure was of secret information and made on a confidential basis. This means that an exemption can be claimed both where there is an express contractual obligation to do so, and also where information is received that the repository knows that the discloser expects it to keep confidential. Material provided to the repository on the basis of non-disclosure until after a certain period of time (or after the provider's death) would seem to fit this definition.

It is also worth remembering that a public authority repository will not necessarily (or, indeed, ordinarily) receive an assignment of copyright in accessioned PDArcs. This raises the risk that in complying with an FOI request, the repository may infringe a copyright held by a third party in the material disclosed. While the disclosure of material in which a 3rd party holds a copyright will not itself be a breach of the CDPA 1998, as there is a statutory defence to infringement where the publication of the material is specifically authorised by an Act of Parliament,[99] copying and distribution of the material by the recipient without permission from the rightsholder would breach copyright.

> The Freedom of Information Act does not place restrictions on how you may use the information you receive under it. However, the Act does not transfer copyright in any information supplied under it. If you plan to reproduce the information you receive, you should ensure that you will not be breaching anyone's copyright by doing so. [100]

A public authority repository would thus be wise to include a general copyright statement in its publication scheme and in any response to a request for information. Such a statement should note that much information made available under the FOIA is subject to copyright protection and that the supply of information under FOI does not give the person who receives it an automatic right to re-use it without obtaining permission from the copyright holder.[101]

---

98 ICO (2007) Freedom of Information Act Awareness Guidance No. 12: When is information caught by the Freedom of Information Act? Version 2.0 5 at p.4-5 http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_12_info_caught_by_foi_act.pdf

99 s.50 CDPA 1988

100 Directgov, Freedom of information http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG_4003239

101 See OPSI (2008) Copyright Guidance: Freedom of Information Publication Schemes http://www.opsi.gov.uk/advice/crown-copyright/copyright-guidance/freedom-of-information-publication-schemes also
National Archives (undated) *The National Archives Publication Scheme: Copyright and the publication scheme*
http://www.nationalarchives.gov.uk/foi/pubschemes.htm

Handling freedom of information risks from the repository perspective

Repository owners will need to have a clear understanding of the freedom of information issues that their particular repository faces, as both failure to disclosure when required to do so, and disclosure in breach of either data protection law or the law of confidentiality will carry reputational and possibly financial implications. This will require a careful risk assessment as early as possible in the developmental process. It is also essential that repository owners ensure that processes are in place to ensure that risk management is an ongoing issue, and that responsibility for undertaking such assessment, as well as developing and administrating methods of handling any risks identified, is clearly located within the staffing structure of the repository.

Current repository trends in freedom of information handling

The current literature with regard to freedom of information and archives/repositories is heavily biased towards FOIA compliance as regards public authority generated records, and there is little mention of materials that have been collected/generated and deposited by private individuals, which are now held by public authorities. However, one important impact of the FOIA which spans that divide is that the Act obliges public authorities to take record keeping and records management seriously. Whilst it would seem logical to assume that archives and repositories have been more likely than most (parts of) public authorities to take such issues seriously, initial surveys suggest that certain aspects of the new regime have caused problems.[102] Areas likely to cause problems with regard to PDArcs include:

- the strict timescale for meeting requests for information (20 working days);
- the need to determine whether DPA 1998 or confidentiality issues are in play;
- handling copyright issues appropriately, including the provision of adequate notification to the requestor as to the rights attaching to the materials released, plus processes for handling complaints that copyright in material released has been breached;
- increased costs associated with meeting FOIA obligations, including staff training, provision of requestor access to materials etc.

Simple freedom of information processes for deposit

Existing processes for negotiating the conditions under which access to PDArcs may be granted, which are appropriate for pre-arranged deposit of limited numbers of 'high profile' PDArcs, are unlikely to be feasible where a repository wishes to accession large numbers of 'digital public' PDArcs. It is likely in those circumstances, that other methods of agreeing appropriate forms of use will be required. These could take the form of simple deposit agreements offering a limited range of disclosure options to the would-be depositor, used in combination with depositor-generated metadata and tagging of PDArc contents. This would require repositories to make clear to depositors:

- the implications of their choice of disclosure options, for access to and reuse of the PDArc;
- the obligations that the FOIA places on the repository, and that these may, in some circumstances, be deemed important enough to the public interest to override the depositor's wishes.

Simple freedom of information processes for access

Repositories will need to consider how they control both access to, and potential reuses of, digital materials from PDArcs under the FOIA, and how they handle the expectations of depositors, third parties who have rights linked to material in a PDArc, and end-users. The provision of information and creation of clear structures for handling potential problems will be vital. Decisions will have to be made about the granularity of the access to PDArcs that have depositor-imposed usage restrictions – does the restriction prevent access to any of the content of the PDArc until the depositor's conditions are met or does it just prevent access to certain information/documents.

---

102 Shepherd, E. (2007) Freedom of Information and Records Management in the UK: What has been the Impact? *Journal of the Society of Archivists* 28(2): 125-138

Does a risk analysis and/or cost vs. benefit analysis suggest it is feasible to adopt a system for 'digital public' PDArcs that is any more complex than "The contents of this PDArc are accessible/ are not currently accessible"?

2.3.2 Information gathering and risk assessments (deposit and access)

Similar criteria apply to information gathering and risk assessment for compliance with freedom of information legislation as applies to copyright and data protection (see above):

- identify current best practice guidelines;
- access and learn from relevant experience derived from existing repositories and projects;
- identify particular issues relevant to:
    - the nature of their repository
    - the specific type of materials they intend to accept
    - the particular type(s) of PDArc depositor and accessor they intend to serve
    - the freedom of information regime
    - the prevailing political and social circumstances;
- assess key issues of concern to depositors and accessors and to develop strategies to reduce the impact of those concerns on the use of the repository.

At this point in time, there does not appear to be a nationally recognised set of best practice guidelines for handling FOIA issues arising from materials that have been collected/generated and deposited by private individuals. However, it appears from anecdotal evidence that repositories and archives have been faced with FOIA questions arising from their existing collections of 'high profile' personal archives, both analogue and digital.[103]

2.3.3 Freedom of Information roles and responsibilities (deposit and access)

Several of the key issues arising from FOIA requirements are dealt with under personal data and copyright above. A public authority repository needs to have some idea of the depositor and third party interests involved in a PDArc in order that it can take suitable measure to protect those interests when dealing with potential accessioning parties under FOI requests. Where depositors have deposited material subject to confidentiality agreements, in principle at least, the repository should not have to review the overall legitimacy of the confidentiality requirement, but it may wish to consider the scope of a particular agreement – is it meant to be a blanket ban on release of material from the PDArc, or can certain information be legitimately released? Where it has received PDArcs which contain third party personal data, it may need to consider whether those third parties should be given the right to object (effectively a s.10 DPA 1998 notice) to the release of that personal data in response to a FOI request. Finally, when releasing material, perhaps as part of its Publication Scheme in the case of PDArcs that are not subject to restraints on public access, or in response to a FOI request where there is no legitimate ground to refuse disclosure, the repository should remind users that having access to the information does not mean having an unfettered right to use it as they see fit – particular documents or other works may still fall within the scope of copyright, and thus cannot be lawfully used without the permission of the rightsholder.

2.4 Liability Issues: Defamation, Contempt of Court, Obscenity and Indecency

The risk that any archive/repository runs when accessioning, preserving and disseminating material that has created and collected by third party depositors, is that lurking within such collections may be materials whose content carries potential liability for possession and/or for dissemination. Such liability may be civil, as in the case of defamation; or criminal, as in the case of obscene and indecent materials; or both as in the case of contempt of court. Traditionally, repositories have sought to identify such materials during the accession process and either remove them from

[103] Part of this FOIA section is based on a response to a query received by the author about FOIA requests relating to the University of Bristol Theatre Collection, which contains archival materials relating to actors, dramatists, directors, and theatres, including personal and professional documents (e.g. letters and records)

collections, or retain them but mark them as unsuitable for general release. This filtering process has often been backed by depositor agreements in which the depositor is asked to warrant that nothing in the collection infringes the rights of third parties and/or exposes the repository to civil or criminal liability. Such processes may work effectively for 'high profile' collections, including PDArcs where there may be considerable discussion between depositor and repository prior to deposit, and where the collection itself may be sorted and catalogued in detail. However, where 'digital public' PDArcs are to be accessioned, the potential number of PDArcs combined with the increasing size of such PDArcs (e.g. digital photograph collections are not limited by the cost of photo-processing) will militate against the use of staff and resource intensive processes, and increase the attractiveness of user-led tagging and filtering. There will still be a role for depositor agreements, although these will need to be designed and drafted to take into account the changing nature of depositors and the deposit process.

Defamation

Defamation law is the communication of a statement that makes a false claim, expressly stated or implied to be factual, that diminishes the public stating of a living natural or legal person.[104]

In most jurisdictions, therefore defamation liability is based on three criteria:

- publication of untrue information about an identified individual, or clearly defined small class of people;
- dissemination of that information to other people than the author;
- damage to the reputation of the person referred to.

The key legislation in this area in the UK is the *Defamation Act 1996*, which was designed to simplify and modernise the law of defamation, in particular with regard to determining who could be sued in a given action.[105] However, national defamation laws vary widely, e.g. Scots law differs in important respects from English law. This is important when considering international Internet interactions, as individuals who believe they have been defamed may be able to choose a favourable jurisdiction in which to sue e.g. where the author of the statement is based, or where the statement was received by others. Thus, a individual defamed on a Usenet news group by a mailing sent by someone in Australia, which is available to users in the UK and US, could potentially choose any of those countries in which to sue.[106]

Under English law, a defamatory statement, or representation, in permanent form is a libel. Statements in books, articles, newspapers, letters, e-mails and webpages are libels, as are statements recorded on tape or other media. For a statement to be libellous, it must:

- be untrue and lower the opinion of the person defamed in the eyes of others – merely abusive statements are not libellous e.g. stating "Respondent B is a moron" is unlikely to be defamatory; falsely claiming that "Respondent B is a creator of child pornography" will be defamatory;
- refer to the person defamed in a way that they are clearly identified;
- be made known to others or 'published' – e.g. the statement is disseminated to people other than its author and the person defamed.

Any living individual can sue for defamation; the dead cannot. A company can sue if the defamatory statement is in connection with its business or trading reputation.

Current interpretation of the law following the Defamation Act 1996 suggests that in respect of a repository:

---

104 For a more detailed overview, see Kenyon, A. (2006) *Defamation: Comparative Law and Practice*, UCL Press

105 *Defamation Act 1996*: http://www.opsi.gov.uk/Acts/acts1996/ukpga_19960031_en_1

106 See further, Collins, M. (2005). *The Law of Defamation and the Internet* (2nd ed.), Oxford University Press

- the display of false information damaging to the reputation of the person referred to in that information, via a publically accessible system, will be considered by the courts to be 'published', and thus libellous;
- the author of a libellous statement captured in a digital object, or written in an annotation, that is accessible to third parties may be sued for damages, unless they did not intend their statement to be published at all;
- if the statement is published within a publically accessible system, such as a repository, which is edited (or moderated), i.e. some other person than the author has control over the content of the statement, or the decision to publish it, that "editor" may be sued for damages;
- if the statement is published within a publically accessible system, such as a repository, by a "commercial publisher" (defined as a person whose business is issuing material to the public, or a section of the public,[107] i.e. there is no requirement of payment by the public) that "commercial publisher" may be sued for damages;
- if the person 'publishing' the statement within a publically accessible system is not an author, editor or publisher, as defined in the Act,[108] or because they are merely involved in "processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form" or acting "as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control"[109] they may not be sued for damages UNLESS
- they failed to take reasonable care in relation to its publication, or knew, or had reason to believe, that what they did caused or contributed to the publication of a defamatory statement,[110] in which case they too can be sued.

It is also worth noting that while s.4A of the Limitation Act 1980 provides that:

> *no action for libel or slander, slander of title, slander of goods or other malicious falsehood shall be brought after the expiration of one year from the date on which the cause of action accrued;*

as far as the courts are concerned, for the purposes of s.4A of the Limitation Act 1980, on-line archives are in effect being continuously republished each time they are accessed. As such, defamatory material made accessible via a repository could be the subject of legal action in England long after the original date of publication, as republication lays the publishers open to legal action every time that the defamatory statement appears.[111]

Contempt of Court

In England and Wales, contempt of court is divided into 'civil' and 'criminal' contempts.[112] Civil contempt relates to circumstances where parties breach an order of court made in civil proceedings, for example injunctions or undertakings. Criminal contempt deals with various actions which would have the effect of interfering with the administration of justice. Criminal contempts essentially fall into five categories:

---

107 s.1(2) *Defamation Act 1996*

108 s.1(1)(a) *Defamation Act 1996*

109 s.1(3) *Defamation Act 1996*

110 s.(1)(b) and s.1(1)(c) *Defamation Act 1996.*

111 See *Loutchansky v Times Newspapers Ltd and Others (No 2)* [2002] 1 All ER 652 (CA)

112 For more detailed overviews, see Miller, C. J. (2000) *Contempt of Court* (3rd ed.) Oxford University Press; Bailey, S. & Taylor, N. (2009) *Civil Liberties Cases, Materials, and Commentary,* Oxford University Press

- publications prejudicial to a fair criminal trial
- publications prejudicial to fair civil proceedings
- publications interfering with the course of justice as a continuing process
- contempt in the face of the court
- acts which interfere with the course of justice.

While the law of the contempt of court was developed by the judiciary through the common law, it was modified by the Contempt of Court Act 1981, although the CCA 1981 neither codifies nor entirely replaces the common law. The CCA 1981 makes it a strict liability offence to publish a '… publication [which] includes any speech writing, broadcast, cable programme or other communication in whatever form, which is addressed to the public at large, or any section of the public'[113] , although this is tempered by the fact that it applies only where such a publication '… creates a substantial risk that the course of justice in the proceedings in question will be seriously impeded or prejudiced'.[114] The statutory 'strict liability' rule is only applied during the period that the case is 'active' and the definition of 'active' is laid down in the Act.[115] However, where an individual knows or has good reason to believe that proceedings are imminent, and publishes material which is likely or calculated to impede or prejudice the course of justice before the point laid down in the Act as the time when the case is 'active' this publication may still constitute a common law contempt.

Examples of actions which would be likely to draw charges of contempt include:

- Publication of material that prejudges the case, especially where it makes the express or tacit assumption that the accused in a criminal trial is guilty;
- Publication of material which is emotive or disparaging, especially where there is an insinuation of complicity or guilt by association;
- Publication of material which is likely to be inadmissible at trial, such as previous convictions, or mention of evidence likely to be excluded as having been improperly obtained;
- Publication of material such as a photograph of the defendant, where the issue of identification forms part of the trial proceedings;
- Publication of material hostile or abusive towards potential witnesses with the intention of coercing them into not testifying, or disclosure of witnesses' names following a court order that their names should not be disclosed if there was a danger that lack of anonymity would prevent them from coming forward;
- Publication of jury deliberations;
- Publication of material breaching reporting restrictions in cases such where in open court there is identification of children involved in the proceedings, or identification of rape victims;
- Publications of material relating to court proceedings closed to the public, including where there is an issue of national security.

Defences to the 'strict liability' offence:

- A person is not guilty of contempt of court under the strict liability rule as the publisher of any matter to which that rule applies if at the time of publication (having taken all

113 s.2 (1) *Contempt of Court Act 1981*

114 s.2(2) CCA 1981

115 Schedule 1, CCA 1981

reasonable care) he does not know and has no reason to suspect that the relevant proceedings are active;[116]

- A person is not guilty of contempt of court under the strict liability rule as the distributor of a publication containing any such matter if at the time of publication (having taken all reasonable care) he does not know that it contains such matter and has no reason to suspect that it is likely to do so;[117]
- A person is not guilty of contempt of court under the strict liability rule in respect of a fair and accurate report of legal proceedings held in public, published contemporaneously and in good faith.[118]

Obscenity

The UK *Obscene Publications Act 1959* (OPA) states that 'an article shall be deemed to be obscene if its effect . . . is, if taken as a whole, such as to *tend to deprave and corrupt* persons who are likely . . . to read, see or hear the matter contained or embodied in it.'[119] The key issues for a jury to consider when assessing particular material are:

- *The possibility of the relevant material being seen as likely to deprave and corrupt*. Could an observer come to the conclusion that some of those who viewed the material might be depraved and corrupted by it?
- *The likely audience for the material*, as this will form part of the assessment of its tendency to deprave and corrupt. When deciding whether material is obscene, an important determining factor is the consideration of whom its likely audience is going to be. This is because some potential audiences are regarded as being more susceptible to being depraved and corrupted than others. Children are seen as an audience that is especially vulnerable in this respect. Thus, material made available in a forum or media that is available to children will be always be subject to stricter regulation than material that is not.

If an article is obscene, it is an offence to publish it or to have it for publication for gain. The *Obscene Publications Act 1959*, as amended by the *Criminal Justice and Public Order Act 1994*, defines a publisher as one who in relation to obscene material:

- distributes, circulates, sells, lets on hire, gives or lends it, or who offers for sale or for letting on hire, or:
- in the case of an article containing or embodying matter to be looked at or a record, shows, plays or projects it, or, where the matter is data stored electronically, transmits that data.[120]

Thus, the transfer of obscene material either manually, by use of computer disks or other storage media, or electronically from one computer to another, via a network or the Internet (e.g. sent by e-mail, or posted to websites), will be caught by the legislation.

The UK *Obscene Publications Act 1964* makes it an offence to have an obscene article in ownership, possession or control with a view to publishing it for gain.[121] As a result, obscene material placed on a webserver will be caught even when an individual simply makes the data available to be transferred or downloaded electronically by others, so that they can access the materials and copy

---

116 s.3(1) CCA 1981, see also *Venables and Another v News Group Newspapers and Others* [2001] EWHC QB 32

117 s.3(2) CCA 1981

118 s.4 (1) CCA 1981

119 s.1 (1) *Obscene Publications Act 1959*

120 s.1(3) OPA 1959

121 s.1 *Obscene Publications Act 1964*

them. In *R v Arnolds, R v Fellows* (1997)[122] the Court held that while the legislation required some activity on the part of the 'publisher', this was provided by the fact that one of the appellants had taken 'whatever steps were necessary not merely to store the data on his computer but also to make it available worldwide to other computers via the Internet. He corresponded by e-mail with those who sought to have access to it and he imposed certain conditions before they were permitted to do so.' However, following the decision in *R v Perrin* (2002),[123] the prosecution will need to show that more than a negligible number of persons likely to be depraved and corrupted would be likely to see the material.

Some UK publishers of obscene material have sought to avoid the reach of UK obscenity law by uploading their material on webservers in other countries. In *R v Waddon* (2000)[124] the defendant prepared the obscene material in England, and uploaded it from England to a website in the US, from which it was then downloaded by a police officer in London. Waddon argued that the material was not published in the UK for the purposes of the OPA 1959, and was thus outside the court's jurisdiction. However, the court held that Waddon was involved both in the transmission of material to the website and its transmission back again to this country, when the police officer gained access to the website – and there was, for the purposes of the OPA 1959, publication on the website abroad, when images were uploaded there; and then further publication when those images were downloaded elsewhere.

In short, a UK-based publisher of digital/online pornographic material featuring adults can be prosecuted for obscenity, if a jury finds the material likely to deprave and corrupt a particular audience. An open access webpage is effectively open to the world, including children, and thus its tendency to deprave and corrupt those likely to have access to it will be high. Publishing the material on a website outside the UK will not bar a prosecution for obscenity, if the material is accessible in the UK. Material open to prosecution need not be image based. In 2008 charges were brought against the author of a blog post detailing the imaginary kidnap, torture and murder of the members of the pop group 'Girls Aloud' (*R v Walker*).[125]

Indecency[126]

With regard to child pornography, the relevant parts of the amended *Protection of Children Act* 1978 (PCA) deal with photographic representations of children under 18 (or persons who appear to be under 18).[127] The Act makes it an offence to take, make, permit to be taken, distribute, show, and possess intending to distribute or show, or publish indecent photographs or pseudo-photographs of children.[128] The Act defines 'distribution' very broadly. It is not necessary for actual possession of the material to pass from one person to another, the material merely has to be exposed or offered

---

122 [1997] 2 All ER 548

123 [2002] EWCA Crim 747 - defendant published a preview webpage, available free of charge to anyone with access to the internet featuring pictures of people covered in faeces, coprophilia or coprophagia, and men involved in fellatio

124 Unreported. Court of Appeal (Criminal Division) 06 April 2000

125 Those charges were subsequently dropped when the CPS accepted that the article could only be discovered by internet users seeking such specific material, rather than it being accessible to people who were particularly vulnerable, i.e. young people who were interested in a particular pop music group – thus there was no audience likely to be depraved and corrupted
See, Girls Aloud in 'murder' blog case, http://news.bbc.co.uk/1/hi/england/tyne/7649231.stm, 2 October 2008
also, Man cleared over Girls Aloud blog, http://news.bbc.co.uk/2/hi/uk_news/england/tyne/8124059.stm, 29 June 2009

126 For a more detailed overview, see Akdeniz, Y. (2008) *Internet Child Pornography and the Law: National and International Responses*. Ashgate

127 The definition of a child was altered from 16 to 18 years' by s.45(1) of the *Sexual Offences Act 2003*

128 *Protection of Children Act 1978*, s.1(1)(a-c)

for acquisition.[129] The PCA also criminalises advertisements which suggest that the advertiser distributes or shows indecent photographs of children, or intends to do so. [130]

The *Criminal Justice and Public Order Act 1994* (CJPOA) amended the PCA adding that 'photograph' shall include:

> data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.[131]

This definition of photograph covers digital representations of physical photographs (thus gif and jpeg image files, downloaded from FTP sites, embedded in webpages, or compiled from Usenet messages, will be treated as photographs)

The CJPOA additionally added the concept of the "pseudo photograph"

> "Pseudo-photograph" means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph."[132]

Thus a pseudo-photograph means any image which is capable of being resolved into an image which appears to be a photograph and, if the image appears to show a child, then the image is to be treated as if that of a child. This means that there is no need for a child to have been used in the creation of the image, indeed the Act covers an indecent image which may not be based on any living subject. The pseudo–photograph amendments deal with situations where, for instance, morphing software is used to create images which look as if they are of children from images of adults.

The *Criminal Justice and Immigration Act 2008* (CJIA) further amends the definition of "photograph".

> References to a photograph also include:
>
> (a) a tracing or other image, whether made by electronic or other means (of whatever nature):
>
> (i) which is not itself a photograph or a pseudo photograph, but
>
> (ii) which is derived from the whole or part of a photograph or pseudo photograph (or a combination of either or both); and
>
> (b) data stored on a computer disc or by other electronic means which is capable of conversion into an image within para.(a)[133]

The term 'indecency' is not defined in either the PCA, or any other statute in which it occurs. In essence, the test would seem to be whether the item in question offends current standards of propriety, or to put it in the American phraseology, whether it offends contemporary community standards. Given that community standards of adult behaviour tend to be rather higher where children are involved, an image involving a naked adult which might be perfectly acceptable, could well be treated as indecent if a child or pseudo-child image were to be portrayed in a similar manner.

The provisions discussed above have clear relevance to activities on the Internet. Placing of indecent pictures of children on a webserver will almost inevitably mean that they will be distributed; when such pictures are held on a computer they can be plausibly said to be in someone's possession; a link to a web site may be considered an advertisement; and an e-mail offering such pictures in digital or paper form certainly would.

A person charged under the PCA with distributing, showing, or possessing intending to show or distribute, has two potential defences:

---

129 s.1(2) PCA 1978

130 s.1(1)(d) PCA 1978

131 *Criminal Justice and Public Order Act 1994,* s.84(3)(b)

132 s.84(3)(c) CJPOA 1994

133 s.69 (3) *Criminal Justice and Immigration Act 2008*

- they did not see the image and that they had no knowledge or suspicion that the image was indecent;
- there was a legitimate reason for possessing or distributing the image e.g. for academic research or in the process of gathering evidence.[134]

It is also an offence to possess an indecent image of a child or indecent child-like image.[135] The defences available include:

- they had a legitimate reason for having the photograph or pseudo-photograph in their possession;
- they had not seen the photograph or pseudo-photograph and did not know, nor had any cause to suspect, it to be indecent;
- the photograph or pseudo-photograph was sent to them without any prior request made by them or on their behalf and they did not keep it for an unreasonable time;
- the defendant proves that the photograph was of the child aged 16 or over, and that at the time of the offence charged they were married, or lived together as partners in an enduring family relationship. [136]

With regard to the computerised making or possession of indecent photographs of children, the UK courts held in *R v. Bowden* (2000)[137] that the intentional downloading and/or printing out of computer data of indecent images of children from the Internet constituted the 'making' of an indecent photograph and was thus an offence under s1(1)(a) of the Protection of Children Act 1978. With regard to the unintentional storage of computer data of indecent images of children in a computer cache the court in *Atkins v DPP* (2000)[138] held that this did not automatically constitute 'making', nor did their possession in a computer cache necessarily mean an offence had been committed under s160 Criminal Justice Act 1988, as the defendant, in such circumstances, must be shown to have known he had the photographs in his possession, or to know he once had them.

In *R v Smith and Jayson* (2002)[139] Smith had received an indecent photograph as an email attachment, and Jayson had browsed an indecent pseudo-photograph on the Internet. In both cases, their browser software automatically saved the images to a temporary Internet cache on their computers. With regard to Smith, the court held that no offence of "making" or "being in possession" of an indecent pseudo-photograph was committed simply by opening an email attachment where the recipient was unaware that it contained or was likely to contain an indecent image. However, when Smith's opening of the e-mail attachment was considered in the light of the evidence relating to his other activities, the court did not believe him to be unaware of the nature of the attachment. Jayson argued that his act of viewing the indecent pseudo-photograph did not constitute the necessary intent to 'make' a photograph or pseudo-photograph. The court, however, held that the act of voluntarily downloading an indecent image from the Internet to a computer screen was an act of making a photograph or pseudo-photograph, as the intent required was 'a deliberate and intentional act with the knowledge that the image was or was likely to be an indecent photograph or pseudo-photograph of a child.'

In summary, a UK-based maker, owner, or publisher, of internet pornographic material featuring children can be prosecuted for indecency, if the jury finds the materials in question contain images of children under 18 (or persons who appear to be under 18) which offend current standards of propriety, and those materials are either photographs, or they appear to be photographs.

---

134 s.1(4)(a)-(b) PCA 1978, also s.1B, added by s.46 SOA 2003

135 s.160 *Criminal Justice Act 1988*

136 s.1(4), s.1A, s.1B PCA 1978

137 [2000] 2 All ER 418

138 [2000] 2 All ER 425

139 [2002] EWCA Crim 683

Downloading and/or storing an indecent image constitutes a 'making of an image' offence. Mere possession is also an offence (except for narrow defences).

Extreme pornography legislation

Under the UK *Criminal Justice and Immigration Act 2008* (CJIA) it is an offence for a person to be in possession of an 'extreme pornographic image'.[140] An 'extreme pornographic image' is an image that:

- is of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal;[141] and is NOT part of a sequence of images which in context are not pornographic;[142]
- AND portrays, in an explicit and realistic way, any of the following;
    - an act which threatens a person's life,
    - an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals (references to a part of the body include references to a part surgically constructed e.g. through gender reassignment surgery),
    - an act which involves sexual interference with a human corpse, or
    - a person performing an act of intercourse or oral sex with an animal (whether dead or alive)
    - AND a reasonable person looking at the image would think that any such person or animal was real
- AND is grossly offensive, disgusting or otherwise of an obscene character.[143]

A person charged under the CJIA for possession of an extreme pornographic image has three potential defences:

- they had a legitimate reason for being in possession of the image concerned;
- they had not seen the image concerned and did not know, nor had any cause to suspect, it to be an extreme pornographic image;
- they were sent the image concerned without any prior request having been made by or on behalf of them, and did not keep it for an unreasonable time. [144]

There is an additional defence for a person charged under the CJIA for possession of an extreme pornographic image where the offence relates to an image that portrays an act which threatens a person's life; an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals; or an act which involves sexual interference with a human corpse and the defendant can prove

- that they directly participated in the act or any of the acts portrayed, AND that the act or acts did not involve the infliction of any non-consensual harm on any person, AND if the image portrays an act which involves sexual interference with a human corpse, that what is portrayed as a human corpse was not in fact a corpse.[145]

2.4.1 Application to Personal Digital Archives

A key point to make about all of the content liability laws outlined above is that either they, or the regulatory regime within which they operate, already make some concessions to what is, in

---

140 s.63 (1) *Criminal Justice and Immigration Act 2008*

141 s.63 (3) CJIA 2008

142 s.63 (4)-(5) CJIA 2008

143 s.63 (6)-(7) CJIA 2008

144 s.65 CJIA 2008

145 s.66 CJIA 2008

essence, a system of 'notice and takedown'. In other words, once a person or organisation hosting the material knows it is illegal, as long as they delete it, or prevent/restrict third party access to it, then their liability will either be significantly limited, or removed altogether. To the extent that this is not the case already, this understanding needs to be incorporated into repository practice, as it will permit a more expansive collection policy, allowing for the collection and preservation of a wider range of material, while ensuring processes in are in place to limit the risk – repositories will not have to catch everything at the borders i.e. at deposit or on access. Working with existing organisations may make this task easier, for example, the Internet Watch Foundation (IWF), a non-governmental charitable body set up by amongst others , UK communications service providers, such as ISPs, mobile phone operators, Internet trade associations, etc. would potentially be in a position to both advise and work with repositories to reduce the risk from child sexual abuse images , criminally obscene pornography and material inciting racial hatred, and to provide an avenue for reporting these to the appropriate authorities if they are discovered.[146]

It is important to also note that there may be legitimate reasons for repositories to collect and preserve materials that are currently considered risky. The normative shifts over time, in areas such as obscenity - *Lady Chatterley's Lover* is probably an acceptable household read today, even for one's wife or servants[147] - mean that failing to capture materials, due to perceived legal risks now, leaves a significant gap in the historical record. After all, what would the history of the Internet, or UK obscenity law, look like without any access to the then 'dangerous' content which influenced it?[148] Clearly there are some lines to be drawn, pictures of child sexual abuse being the obvious example (although jurisdictional differences over what is, and should be, labelled as 'child pornography' vary significantly).[149] However, as examples such as the police raids on Manchester bookstores in the 1990s (ordered by the then Chief Constable James Anderton, whose outspoken attacks on homosexuals earned him the sobriquet 'God's Cop') over material sold elsewhere in the UK without comment,[150] or the Mapplethorpe controversy at the University of Central England in Birmingham in 1998,[151] graphically demonstrate, libraries and repositories may face some legal risks even when dealing with material which is viewed by many as legitimate content. Repositories have always held some risky content, even if at the time of its collection it was deemed unsafe or unacceptable to make it publicly available. There is some risk that the novelty of applying legal regimes to digital content may mean that they end up being perceived by repositories as greater risks, and that they thus are treated in a different way to which analogue materials of a similar type would be handled. The degree to which our digital archives should be 'sanitised' on the

---

146 Internet Watch Foundation
http://www.iwf.org.uk/

147 In *R v Penguin Books Ltd* [1961] *Crim LR* 176 (the Lady Chatterley case) prosecution counsel Mervyn Griffith-put the question to the jury "Is it a book you would wish your wife or servants to read?"

148 See, e.g. Johnson, P. (1997) Pornography Drives Technology: Why Not to Censor the Internet. *Federal Communications Law Journal* 49(1): 217-226

149 Some countries consider child pornography to include material involving persons under the age of 18, others have set the level at material involving persons under the age of 16. Some countries criminalize creation, offering, dissemination, procuring and possession of child pornography; others restrict criminalization to creation, offering and dissemination. Some countries require evidence that an actual minor was involved in the creation of the pornography, others also criminalize materials that appear to involve a minor (e.g. where a person over the age of 18 pretends to be under 18, or where innocent images of minors are merged with pornographic images), and/or images that depict minors engaged in sexual activity (e.g. sketches or comic strips)

150 Petley, J. (1996) "Savoy scrapbook", *Index on Censorship*, 25(1): 162-166

151 In June 1998, British police seized a book, Mapplethorpe, from the stock of the library at the University of Central England in Birmingham. The book contained photographs of homosexual activity and bondage scenes taken by the internationally renowned photographer and artist Robert Mapplethorpe. Despite the fact that the book was widely acknowledged as serious artistic work, the police initially told the University that its contents might contravene the Obscene Publications Act 1959. The Crown Prosecution Service, however, declined to bring a case. Charlesworth, A. (2003) n.32 at 17

grounds of preventing legal risk, should not outstrip the 'sanitisation' of paper archives. Indeed, with the advent of legal deposit for a wide range of digital materials, including PDArcs, this might be an opportune moment for a reappraisal of existing policy in this area. This exercise could, amongst other things, have as an aim the provision of information and guidance to legislators about the impact of existing and proposed legislation on the ability of repositories to perform their task of providing future researchers with as wide a range of contemporary materials as possible.

2.5 Law, Pragmatism and Policy

As can be seen from the foregoing, there are a range of legal issues that public repositories need to provide for in their policies, processes and deposit licences for accessioning PDArcs. Of these issues, copyright and data protection/privacy pose the highest profile legal risks, although freedom of information is likely to play an increasing role in public archives' and repositories' workload, particularly where the PDArcs of high profile depositors are involved. However, these are already issues with practical implications - even institutions that are not actively seeking digital media are already receiving them - as, for example, a series of floppy disks among boxes of papers, or on the hard disks of personal computers.

The current approach to digital objects that appear in personal archives remains quite conservative. The prevailing attitude appears to be that it makes sense to keep one's legal exposure low, even though this may have the effect of limiting widespread access to a resource. Making a digital object available in a single computer system in a reading room may not protect a repository from legal action, but it will limit the potential scope of that action. This conservative approach is fostered by the relative paucity of caselaw in this area, which means there is a lack of certainty about how the judiciary will interpret existing legislation in a given situation.

In practice, if a repository adopts effective processes to reduce the risks to individuals' rights attendant on making public disclosures of personal digital objects, and is transparent about its reasons for disclosing material in a particular way, then it seems clear from the activities of other repositories, e.g. the Internet Archive, that risks can be significantly reduced – what they cannot be is wholly removed, in the absence of clear legislative or judicial authority on that point. This is the position that appears to be developing throughout the digital environment – a pragmatic recognition that a conservative interpretation of the law in areas of rapid technological change is a 'safe' option, but at the same time also a negative influence in obtaining and preserving valuable material.

Adopting a less conservative, but still balanced and pragmatic, policy may run the risk of an encounter with an unsympathetic court - but where there are significant public benefits to be gained (in this case in the social value obtained through the capture and public reuse of personal digital objects), the fact that such a policy exists provides a court with a plausible rationale for construing that social value as outweighing the value in permitting the absolute exercise of individual legal rights over digital objects. The current discussion surrounding the Google Books repository is a case in point. It has pushed forward current legal thinking on the acceptability of new methods of enhancing access to, and use of, out-of-print works, even where the methods adopted by Google may presently technically breach copyright.

For a repository, dealing consistently and effectively with the legal issues raised by the accessioning of PDArcs, both at start-up and during operation, will require the clear allocation of responsibility for those determining and addressing those issues within the repository's management team. That responsibility will span both the deposit and user access functions of the repository, as any changes to policy on the one side will almost inevitably have repercussions on the other. It is important that processes are in place to ensure that risk management is an ongoing issue, and that responsibility for undertaking such assessment, as well as developing and administrating methods of handling any risks identified, is clearly located within the staffing structure of the repository. Effective legal risk management is key to establishing and maintaining both depositor and user trust in the reliability of a repository. In short, building a flexible legal policy framework, based on an initial background

and risk assessment, which contains clear and documented processes for deposit and access management, policy and process audit and risk amelioration, and which incorporates the ability to effect coherent change management in the light of shifts in environmental factors, will be essential for long-term sustainability.

While this may sound time-intensive, the amount of work/cost involved in putting into place a system which can both express a repository's legal policies for deposit and access of PDArcs, and provide contextually effective deposit licences, via a number of layers of complexity (see below), is likely to be minimal compared to the benefits accrued in terms of both depositor/end-user understanding and potential future repository interoperability. For many users, particularly professional researchers, a clear understanding of the legal issues relating to their use of materials from a particular repository will often be central to their willingness to utilise it, and to their effective and legal use of items from it. Presenting a clear policy statement outlining those issues will permit a repository to make definitive statements about depositor/repository roles, including where the responsibility lies for establishing which legal issues apply to particular deposited items, and the effect those legal issues will have on access to, and use of, those items.

Layering of policy documents, deposit agreements and end-user agreements

'Layering' is a technique increasingly used in data protection circles for privacy policies, and also by the Creative Commons for its licence scheme. The concept of policy 'layering' envisages a set of policy explanations which cover the same policy principles, but which are targeted at particular sub-sets of audience, in terms of technicality of explanation, or length of explanation, and often both.

In data protection terms, privacy policies are often aimed at lay readers, interested parties and experts. The lay readers are assumed to be simply interested in a very basic explanation of what the policy means for them. The interested parties are assumed to want to know more about the wider implications of the policy and how it affects them in detail. The experts are assumed to want chapter and verse on the precise nature of the policy and how it relates to the Data Protection Act 1998.[152]

The layered licences used by the Creative Commons take a slightly different approach. When you create a licence using the Creative Commons licence generator, the program produces three versions of the licence:

- *Commons Deed*. A plain-language summary of the licence, complete with the relevant icons.
- *Legal Code*. The fine print that you need to be sure the licence will stand up in court.
- *Digital Code*. A machine-readable translation of the licence that helps search engines and other applications identify your work by its terms of use.[153]

A layered policy or user licence/agreement, if both accurate and well designed, is thus an effective way of communicating an appropriate level of information to a particular audience. This technique would work equally well for many types of deposit agreement, with the degree of complexity of agreement required by the depositor being determined partially by virtue of the repository's own risk assessment, but largely by virtue of the risk factors that depositors themselves allocate to the material being deposited.

3. Personal Digital Archives and Ethics

The design and application of ethical standards to the collection, archiving and making available of PDArcs, will require careful thought, particularly if public repositories seek to collect PDArcs from a wider range of sources, including publicly available online sources. Ethical standards are often

---

152 See, e.g. Center for Information Policy Leadership (2007) *Ten steps to develop a multilayered privacy notice* http://www.hunton.com/files/tbl_s47details%5Cfileupload265%5C1405%5Cten_steps_whitepaper.pdf

153 Creative Commons, License Your Work http://creativecommons.org/about/license/

reflected in the law, but organisations may choose to set themselves higher ethical standards than the law strictly requires. In such circumstances, legal requirements form the baseline of ethical requirements; they set a standard below which the actions of the organisation may not fall. The task for public repositories is thus to both understand where their proposed activities may breach the law, and to identify where the mere observance of the law is insufficient to meet their designated ethical standards. There is also scope for public repositories to collaborate in the setting of ethical standards, in order to facilitate efficient interoperability and interchange of materials without compromising public trust.

3.1 Ethical Standards in Changing Social Environments

As has already been noted, the development of PDArcs, both formal and informal, is taking place in a social environment that is undergoing considerable change. Conventions about the acceptable use and reuse of content, including those conventions captured in copyright law, are being fractured by the increasing public ability to share and reuse content. Conventions about the privacy of the individual, including those conventions captured in privacy, confidentiality and data protection laws, are being undermined by the online social networking, 'reality' TV, and government data collecting, sharing and mining. These factors, combined with a public expectation of rapid access to digital materials, and the increasing expectation that information held by public bodies will be made available on demand, are creating an environment where the ethical standards applied to the collection, archiving and making available of analogue personal collections are increasingly under pressure.

Thus, if a PDArc is deposited with a public archive or repository, the expectations of the public about:

- the time period within which that resource will be become available for third party access,
- the degree of access to all elements of that resource, and
- the ability of third parties to use or reuse elements of it,

will increasingly be different from the previous expectations about a paper-based personal collection. In such circumstances, the role of public repositories in defining a clear set of ethical standards with regard to PDArcs becomes important, not just in terms of institutional policy, but also in terms of helping to set the normative standards for future expectations about access to such materials.

It is important to emphasise to would-be users of personal collections, whether paper-based or digital, that deposit of such collections has almost always been undertaken on a voluntary basis and, at the very least, even where consent is not formally sought, it will be important that deposit/accession is not opposed by the creator of the PDArc, or the holders of any rights in the works in the PDArc. It is thus vital that existing types of trust relationship between repositories and would-be depositors are maintained. If such trust relationships break down, then archives and repositories may find it harder to obtain voluntary deposits, and face increased opposition to any moves to obtain UCC/PDArc material from commercial operators.

3.2 Outlining the Ethical Issues

PDArcs may contain an array of material - personal correspondence, legal and financial papers, personal and family papers, drafts of publications, publications. It is likely that in the longer term, the 'traditional' materials will be increasingly accompanied by sound recordings and video. The material in question will relate not just to the individual who has created the collection, but may also contain information about a significant number of other individuals. The primary ethical consideration will be to ensure that these individuals are protected as far as is possible from:

- potential physical or psychological harm, discomfort or stress, and
- damage to their personal social standing, privacy, personal values and beliefs, their links to family and the wider community, and their position within occupational settings,

as a result of the PDArc being accessioned by a public archive or repository, and eventually made available to third parties. Additionally, the depositor of a PDArc and, as appropriate, other affected parties should be made clearly aware of the purposes to which the PDArc or elements of it may be put, and the extent to which they can object to, or prevent, any of those purposes at any time.

There may also be ethical considerations with regard to the effective protection of rights in any of the content of the PDArc. While, for example, copyright law would, in principle, protect the copyrights of those whose works are contained in a PDArc, in practice such rights may be difficult to enforce effectively if the works are permitted to 'escape' the archive or repository. Thus, the archive or repository may have an ethical obligation to ensure that the legal rights of those with interests in the PDArc are not subverted by virtue of particular access practices and policies. This may in turn lead them to consider the extent to which it is feasible to place meaningful ethical constraints upon their users, whether through mechanisms such as ethical committees (e.g. for academic researchers), or via contractual requirements in access agreements.

3.3 Designing an Ethical Approach to Personal Digital Collections

When creating policies and processes for the collection, archiving and making available of PDArcs, public repositories will need to consider:

- what information should be provided to depositors concerning the ethical issues surrounding deposit of PDArcs
    - e.g. information about privacy and data protection risks; the possible effects of deposit on depositors and third parties; the ability (or otherwise) of a depositor to control use of the PDArc, including the ability to withdraw some or all of a PDArc from the archive/repository; the ability of third parties to request removal of some or all of a PDArc from the archive/repository
- how information will be most effectively provided to depositors, about what may be done with the contents of their PDArc, in advance of the deposit of PDArcs being made, through whichever channels the archive/repository is seeking to use in order to accession material
    - e.g. for 'high profile' PDArcs, information can be provided both in written form and verbally in discussion with representatives of the archive/repository. The high level of interactivity will allow depositors to gain a clear picture of the purposes to which their PDArc will be put
    - e.g. for 'digital public' PDArcs collected by voluntary deposit with the archive/repository, information can be provided in paper form or electronically prior to the depositor signing a deposit agreement. While face-to-face discussion with representatives of the archive/repository would be less likely, the ability for depositors to ask questions via interactive website or e-mail could be considered
    - e.g. for 'digital public' PDArcs collected by agreement with a commercial social networking provider, information can be provided electronically, prior to a user being asked for permission for the archive/repository to automatically archive their materials via the commercial social networking provider. While there would be no face-to-face discussion with representatives of the archive/repository, the ability for depositors to ask questions via interactive website or e-mail could be considered
- which polices and processes will be in place to ensure that ethical considerations are properly applied to the collection and use of PDArcs by the archive/repository's staff and users
    - e.g. measures to ensure that appropriate levels of confidentiality and security are applied to each PDArc, and that these measures are made known to both staff and users, and that they are effectively enforced.

When considering ethical policies and processes, an archive/repository will need to have an understanding of the legitimate expectations of their depositors, and other third parties, about the

appropriate and agreed uses of the contents of the PDArc. As noted above, at the start of this section, shared understandings in this area will clearly help to facilitate trust and interoperability between repositories, and between repositories and their users.

4. Assessing Solutions to the Issues raised by Personal Digital Collections

As with analogue personal collections before them, PDArcs raise numerous legal and ethical issues that archival organisations must address, if those PDArcs are to be appropriately and effectively utilised by future researchers. Many of those issues are essentially identical for analogue personal collections and PDArcs. Where differences start to emerge, they do so because of:

- the range of types of PDArc that now exist, from the traditional collections of eminent persons to the collections of 'ordinary' people (members of the digital public), the latter largely available because of the storage capacity of digital media, and the readily availability of tools with which to create and capture content and information for posterity;
- the involvement of commercial entities in providing the technology and support for the creation and maintenance of PDArcs;
- the ease with which digital data can be accessed, stored and copied;
- the expectations of the public about how, where and when PDArcs should be accessible, and for what purposes.

Technology frequently runs ahead of existing laws and ethical guidelines, and even though the law may subsequently be changed to adapt to changed circumstances there is almost inevitably a timelag; moreover, the subsequent changes in the law that emerge may well not be quite as initially supposed. As a result, at least some of the solutions to those problems are likely to lie outside traditional approaches to handling legal and ethical issues.

4.1 Collecting Data about Data: The Role of Metadata (Code)

A problem common to both analogue personal collections and PDArcs is that of determining the legal criteria applicable to the use of each part of the collection. Indeed, access to material in a PDArc may need to be determined on a file-by-file basis, due to differences in legal protection periods for copyright purposes, the need to avoid disclosing data which is protected under privacy or confidentiality law, or the need to avoid disclosing information which may expose the depositor, or the archive/repository, to action for defamation.

A vital element in ensuring the most efficient accessibility of material in a PDArc, whilst avoiding unlawful or unethical disclosures, will be the collection and storage of metadata pertinent to that material, ideally in a fashion which permits the effective automation of the process of determining when material should be made available.

Metadata can, however, be a problematic issue. This is primarily because the metadata that are likely to be required are rarely created at the same time as the material to which they relate (this may change in the future, and there can be a significant amount of embedded metadata in files which are not immediately apparent to the user) Often repositories must create metadata for material upon accession. Where a PDArc contains a large number of files, this process can be time-consuming and expensive. While such investment may be seen as both worthwhile and feasible for small numbers of 'high profile' PDArcs, e.g. those of an author, or a politician, attempting to scale a bespoke metadata process up to handle large numbers of 'digital public' PDArcs, whether these are deposited directly, or collected via a commercial service, is likely to be impractical.

Thus, if greater deposit of PDArcs is sought, archival organisations are likely to have to look to depositors to have created at least a basic set of metadata for the files in their collection. Facilitating this will require a number of things:

- a simple and easy to apply metadata schema, preferably in the form of a simple program that can generate the actual metadata from information entered into a GUI by a user. An agreed metadata schema for PDArcs across repositories would permit greater interoperability between them;[154]
- basic information for would-be depositors about the purpose of metadata and its importance in the collection, archiving and making available of PDArcs by archives and repositories, in ways that protect both the depositor's and the repositories' interests;
- the provision of incentives to encourage would-be depositors to use the metadata system – for example, for 'digital public' PDArcs, perhaps making it a requirement of acceptance by an archive/repository.

There has been some scepticism in the archive and repository community that user-generated metadata will be an effective means of attaching relevant and accurate information to digital objects. To date, experiments with requesting/requiring user-generated metadata in areas such as e-learning material repositories suggest that user interaction with metadata processes has been patchy at best. On the other hand, it has been argued that users are becoming increasingly accustomed to adding metadata to materials by virtue of the ability to interact with objects on Web 2.0 sites, e.g. by tagging.

Regardless of the current state of user-generated metatagging, creating an effective system for creators and depositors of PDArcs to use to make legal statements about files in their collections, would significantly reduce the current ingestion time required by repositories for new PDArcs. Embedding an understanding of the importance of metadata creation would also help to ensure that creating metadata became part of the routine process of creating a longstanding and richly useful PDArc.

4.2 Making Deposit a PR Success: Involving Community (Norms)

Another problem common to both analogue personal collections and PDArcs is the fact that potentially interesting collections are often unstructured and 'unfiltered', that is to say they contain significant amounts of material which is not suitable for deposit, or which will not be required by the archive/repository. This is more likely to be the case for informal PDArcs (e.g. a profile stored on a Web 2.0 service), than it is for 'posterity' PDArcs, as an individual creating the former is less likely to be thinking in terms of deposit, as opposed to current utility, when creating the collection.

The rise of digital UGC provides an opportunity for archival organisations to influence current practices. As more people create digital content, or build PDArcs, so they have more of a personal 'investment' in what they have created. They are also more aware of the potential benefits of having electronic access to both their aggregated content, and to the aggregated content of others – consider the growth in interest in researching personal and family histories that has been fuelled by the accessibility of online genealogical materials.

Public repositories are in a good position to take advantage of these developments, by virtue of their ability to provide long term, archiving access and preservation for PDArcs – services which are unlikely to be supported by 'free' Web 2.0 services. Targeting the 'community' of personal digital collectors with the promise of such services for PDArcs that are effectively structured and filtered, and which contain basic metadata about the files within them, would add an incentive for collectors to utilise tools/processes which would facilitate deposit, including ensuring a higher standard of legal metadata.

---

154 Charlesworth, A. Ferguson, N. Morgan, E.L. Schmoller, S. Smith, N. & Zeitlyn, D. (2008) *Feasibility study into approaches to improve the consistency with which repositories share material*. Project Report, JISC, 5 November 2008 http://ie-repository.jisc.ac.uk/256/1/jisc-clax-final-report-repocon.pdf

Additionally, there is also an important role for repositories to bring clarity to the legal and ethical issues surrounding deposit of PDArcs. This would permit them to demonstrate that when effective legal and ethical measures are in place, providing the appropriate level of protection required by a depositor, then participation in the deposit of PDArcs can have important social benefits with little risk to the individual. Such benefits might be focused broadly, e.g. the preservation of the digital cultural history of the UK, or more narrowly, e.g. the facilitation of the extraction of valuable research information from one or more PDArcs.

4.3 Leveraging Web 2.0: Involving Commerce (Market)

The rapid development of social networking services and other Web 2.0 data storage services provides another access/influence point for public archives and repositories. Until recently, the marketplace for tools to facilitate the creation of personal digital collections seems to have been relatively small. This may well be because of the heterogeneous nature of user creation and storage of digital works:

> There seems to be many distinct styles of conducting digital lives. Our research [The Digital Lives Research Project] found significant differences in:
>
> - Methods and places of storage;
> - Familiarity and expertise with hardware and software;
> - Understanding of the meaning of a 'personal digital collection' … ;
> - Individual perceptions of what and especially how much is worth keeping (as is the case with conventional archives too);
> - Relative values attached to digital and analogue items.[155]

This appears to have militated against the development of particular tools for personal digital collections, and, in turn, against the development of standards, such as metadata standards, that would aid in the deposit, archiving and making available of PDArcs.

The development of Web 2.0 storage services has the potential to worsen the fragmentation of personal digital collections, by spreading digital objects across a range of services. However, they also provide a potential gateway for the provision of tools for structuring PDArcs, as users search for ways both to keep track of their digital objects across those services, and on their own equipment, and to provide/retain context for those objects. Yet such tools face potential problems:

- Where is the impetus to develop them going to come from? Individual Web 2.0 services may have no particular incentive to provide a tool which maps the location of elements of a personal digital collection within a user's own equipment and across numerous online services.
- Even if a user's data can be mapped across numerous online services, can all of the desired information be accessed and extracted for the purpose of maximising the usefulness and research value of a PDArc? Users and archivists may find it more difficult to extract digital objects from Web 2.0 services than it was to upload them. This problem will be exacerbated where access to the digital object is protected by password.

Is there a role for repositories in addressing this issue? Certainly, there would be significant advantages to being involved in the development of such tools, and being able to provide input to defining what information a PDArc mapping tool should contain (e.g. effective metadata for each digital object). There may also be the ability to drive a new market for such a tool, by raising user expectations as to how their PDArcs/PDArc tools could increase the value of their digital objects to them, and at the same time increase the likelihood of their PDArc being accepted for archiving for access by future generations.

---

155 Williams, P. Dean, K. Rowlands, I. & John, J.L. (2008) Digital Lives: Report of Interviews with the Creators of Personal Digital Collections, *Ariadne* 55, 30 April 2008 http://www.ariadne.ac.uk/issue55/williams-et-al/

In terms of facilitating the collection of personal digital objects and PDArcs, archival repositories could seek to work more closely with commercial services which host digital objects/PDArcs. As noted above, commercial services may not have an incentive to retain digital objects/PDArcs in the long term, or may only take the cream, the most obviously and immediately rewarding personal objects. However, if the commercial services were to obtain appropriate permissions from their users at the time of the deposit of the digital objects/PDArcs with them, then it should be possible to develop a system whereby digital objects/PDArcs can be collected legitimately from commercial services for archival purposes.

For example, a user wishes to create an account on a social networking site. As part of the account creation process, the user is asked whether they are willing to allow the digital objects they place in the account to be collected by an archive/repository and, subject to terms and conditions that are made available to the user at that point, for those digital objects to be preserved for future use/research. This could be an 'opt-in' or 'opt-out' process. 'Opt-out' would probably result in the collection of more material, but 'opt-in' would be more in line with current privacy/data protection trends. Such a collection process could be made attractive to both the commercial services and their users. Users would have the opportunity to have their material preserved for posterity by a trusted third party (the archive/repository), and this could be a potential marketing device or service distinguishing factor for commercial services.

4.4 Keeping it Simple Successfully: Letting Non-lawyers use Rules (Law I)

While there are legitimate concerns amongst archivists about the legal risks posed by accessioning PDArcs, for the vast bulk of digital objects in a PDArc the actual legal risks (i.e. the chance that the collection, archiving and making available of the digital object will trigger a legal action or threat of legal action) are very low. In many cases, the collector or depositor of the PDArc will be aware of the items within it that might pose such legal risks either at the time of creation/incorporation, or upon deposit. For 'digital public' PDArcs it would seem practical to allow the depositor to firstly make that determination, and secondly to flag the digital object accordingly. As noted in 4.1, this could be achieved by the use of a metadata schema. However, a simpler approach might be one drawn from/allied to the Creative Commons project. Here, the depositor could flag digital objects (or groups of digital objects) within the PDArc with a set of icons to provide a simple user-friendly device to alert either archivists or potential third party users of the digital object to any legal risks or restrictions.

Examples

Icon/Symbol	Meaning	Possible additional data
© Me	Depositor created/owned work	Type of work
© 3rd	Third party owns copyright	Identity of 3rd party; Type of work
© Mixed	Copyright is owned by more than 1 person	Identities of parties; Type of work
DP Me	Contains Personal data of Depositor	
DP Me *	Contains Sensitive Personal data of Depositor	Type of sensitive personal data
DP 3rd	Contains 3rd Party Personal data	
DP 3rd *	Contains 3rd Party Sensitive Personal data	Type of sensitive personal data
Confid 10	To be kept confidential for 10 years	Reason for confidentiality
Confid Death	To be kept confidential until depositor's death	Reason for confidentiality
	Material the depositor considers to pose a risk not otherwise indicated	Perceived risk

As with all such 'self-certification' schemes, there is a risk that depositors will fail to use the system at all, or will inaccurately flag their digital objects. However, if this system is used with 'digital public' PDArcs then occasional failures should not significantly increase legal risk, in the

same way that 'notice and takedown' processes for ISPs don't work 100% percent of the time, but reduce their legal risk to manageable levels. This approach, in conjunction with a deposit agreement which places the onus upon the depositor to ensure that the digital objects deposited do not infringe the law, would form part of the risk amelioration process for items perceived as low risk.

4.5 Immovable Objects: Personal Digital Collections and Law Reform (Law II)

As ever, in such circumstances, the ideal solution to legal problems raised by the collection, archiving and making available of PDArcs by public repositories would be to effect suitable changes in the law to permit them to do so without risk of incurring legal sanction by parties other than the depositor (for breach of any conditions the depositor might have placed on the use of the PDArc). They would still need to consider the ethical risks of their activities, but blanket immunity, or immunity subject to a form of 'notice and takedown' (such as that provided to Information Society Service providers (ISSPs) under the eCommerce Directive[156] in national implementations like The Electronic Commerce (EC Directive) Regulations 2002[157]), would vastly increase the potential material that could be accessioned. Regrettably, the UK government has shown little interest in facilitating the preservation of British digital history in this fashion at any speed, although moves are, belatedly, afoot.[158] Different approaches can be seen in Scandinavia where digital repository activities, such as large scale web archiving, have already been facilitated by legislative intervention in countries such as Sweden,[159] Denmark[160] and Finland,[161] and it is likely, from a copyright perspective at least, that those jurisdictions will be in a better position to tackle the issue of PDArcs.[162]

Although the Legal Deposit Libraries Act 2003 (LDLA)[163] put in place processes for the inclusion of a wider range of electronic materials in the legal deposit process,[164] progress has been slow. The Legal Deposit Advisory Panel (LDAP)[165] which advises the Secretary of State on the timing and

---

156 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF

157 The Electronic Commerce (EC Directive) Regulations 2002 http://www.opsi.gov.uk/si/si2002/20022013.htm

158 See Tuck, J. Web Archiving in the UK: Cooperation, Legislation and Regulation *Liber Quarterly* 18 (3/4) http://liber.library.uu.nl/publish/issues/2008-3_4/index.html?000258

159 The Swedish government issued a special decree in May 2002, with regard to the work done by the Royal Library in acquiring, preserving and making accessible everything found on the Swedish Internet. The decree authorizes the Royal Library to both collect material from Swedish web sites on the Internet and also to allow public access to it within library premises

160 Act on Legal Deposit of Published Material (Unofficial Translation of Act No. 1439 of 22. Dec. 2004) s. 8-11 http://www.kb.dk/en/kb/service/pligtaflevering-ISSN/lov.html

161 Jacobsen, G. (2008) Web Archiving: Issues and Problems in Collection Building and Access *Liber Quarterly* 18 (3/4) http://liber.library.uu.nl/publish/issues/2008-3_4/index.html?000273

162 The Scandinavian countries have a stronger data protection culture than the UK (see e.g. C-101/01 *Lindqvist* [2004] 1 C.M.L.R. 20) and the strict approach adopted may hamper the reuse of PDArcs more than the issue of copyright. See Jacobsen, *ibid*

163 The Act received Royal Assent on 30 October 2003 and came into force on 1 January 2004. See The Legal Deposit Act 2003 http://www.opsi.gov.uk/acts/acts2003/ukpga_20030028_en_1

164 See Field, C. (2004) `Securing digital legal deposit in the UK: the Legal Deposit Libraries Act 2003', *Alexandria* 16(2): 87-111

165 The Legal Deposit Advisory Panel was established as an Advisory Non-Departmental Public Body in September 2005. It comprises fifteen members: five librarians, five publishers, and five independent members, and is chaired by Dr Ann Limb

content of regulations relating to legal deposit did not meet until late 2005, and there was initially little evidence of significant advances in grappling with the sorts of issues that UGC and PDArc pose for the role of Legal Deposit libraries in acquiring, preserving and giving access for the long term to the cultural, intellectual and national heritage of the UK. Even the capture of websites of interest, where the owners of copyrights have granted permission for their website to be archived, remains, to date, a slow process limited by a lengthy, time-intensive permissions process.[166]

In some respects, the LDLA 2003 appears as a classic example of legislation that was outdated even before it reached the statute book. It was still largely focused on traditional publishing ventures transferred to electronic media (CD-ROMS and microforms, ejournals), and while it provided some degree of immunity to deposit libraries from copyright infringement and content liability, the applicability of this to both web harvesting and the accession of UGC and PDArcs appears limited under the statute itself. As such, at present (and subject to future developments by Regulation under the LDLA 2003, discussed below), the ability of even Legal Deposit libraries to accession online or offline PDArcs without incurring legal risk is not significantly improved by the LDLA 2003.

Recent developments, however, suggest that the long term future for electronic archiving may be brighter. Following the publication of a LDAP commissioned report on the types of electronic publications that might be subject to e-legal deposit,[167] which suggested:

> … a new taxonomy based not on the traditional print-world formats such as books, journals, newspapers, maps, etc but rather on categories such as online/off-line; content delivered to/ collected by users; freely available content/content protected behind a barrier[168]

it appears that the LDAP may be willing to adopt a broad regulatory stance to the legal deposit of a wide range of digital objects – if this is the case, this is to be welcomed. Additionally, in mid -2008, the LDLP considered the issue of free online publications:

> …three options have been assessed and costed:
>
> 1. permissions-based harvesting and archiving (this is where explicit permission has to be gained from a Web site owner before a Web site can be harvested and it is the model used by UKWAC) [9];
> 2. regulation-based harvesting and archiving; and
> 3. archiving left to the market.
>
> After full analysis and costings, these options were put to LDAP in May 2008, together with a recommendation for the full Regulation option. The full Regulation option would allow the legal deposit libraries in the UK to harvest, preserve and make accessible this category of material without the need for permissions but within certain restrictions laid down by the Act, for instance, access to the content on legal deposit library premises only. At the same time the Act affords publishers and libraries protection on copyright infringement and defamation.
>
> It is estimated that this Regulation-based approach, not requiring permissions, would be much more cost effective than the UKWAC permissions approach. In comparison with the approximately 3,000 sites so far collected by UKWAC, it would enable whole UK domain harvesting and would

---

166 See the UK Web Archiving Consortium http://info.webarchive.org.uk/aboutthearchive.html and Tuck, J. (2006) Collecting, selecting and legal deposit (PowerPoint presentation) 12th June 2006 http://www.dpconline.org/docs/events/060612Tuck.pdf

167 Powell, D. (2006) *Refining the map of the universe of electronic publications potentially eligible for legal deposit*. Report commissioned by the Legal Deposit Advisory Panel http://www.culture.gov.uk/images/publications/EPS_Report_to_LDAP_Nov_2006.pdf

168 Milne, R. & Tuck, J. (2008) Implementing e-Legal Deposit: A British Library Perspective *Ariadne* 57 http://www.ariadne.ac.uk/issue57/milne-tuck/

In these circumstances, "behind a barrier" would be widely understood to mean works available to the public, but subject to access only if certain conditions, e.g. payment of a fee, membership of an organisation etc, are met. Subscription e-journals would fit this description. It would not normally cover personal digital objects restricted to the individual or to their friends and family

secure an estimated 80% of the domain for the national published archive after 10 years at a current annual cost of £215 per terabyte. LDAP accepted this recommendation, subject to clarification of one or two points.[169]

It has been suggested that if this approach is accepted by the Secretary of State for the Department for Culture, Media and Sport, then a Regulation putting this recommendation into effect could be in place by as early as late 2009.[170] This would be a major shift towards effective collection of web-based materials and would also be a significant step towards enabling the automated collection of online components of PDArcs. It should be noted however that despite some specific legal protection, with regard to copyright and defamation, legal deposit libraries would still need to carry out legal risk assessments and consider appropriate amelioratory strategies. The protections would also be limited to the legal deposit libraries.

What then might suitable UK legislation to enable repositories to effectively capture PDArcs look like?

- Ideally, there would be a move away from the concept of 'legal deposit', bound as it is to concepts of traditional style printing and publication that are inimicable to the effective preservation of many digital objects – the focus of legislation would thus be expanded to provide a legal basis for other forms of acquisition of digital objects – **a change in focus from the print environment to encompass both print and digital objects**
- Recognition that the cultural, intellectual and national heritage of the UK is reflected or expressed in very different ways in the 2000s would mean the removal of the focus on traditional forms of publishing, and the granting of the ability to collect/harvest/accept the deposit of, and archive, a much wider range of digital materials than currently permitted, including all forms of digital object. This would remain subject to certain controls, such as the fact that digital objects should have a connection with the United Kingdom - but would not require that permission be sought from rightsholders in advance – **broad application of the legislation to digital objects generally.**
- While the Legal Deposit libraries would almost certainly wish to retain their privileged status, it is also likely, given the time and cost involved in accessioning digital objects and PDArcs, that they would wish to be able to easily delegate powers in certain areas to other 'authorised' organisations, including smaller archives and libraries, to collect, archive and make available those types of material. Authorisation would be conditional upon the institution in question demonstrating that they had
    - appropriate risk assessment and risk management strategies
    - appropriate ethical guidelines and practices

  and institutions would be subject to audit on these issues, by the authorising body, on a regular basis – **efficient capture of, and access to, PDArcs and digital objects within a clear legal and ethical framework.**
- Immunity could be granted to authorised archives and repositories from liability for copyright infringement, or any other content liability, in materials contained in PDArcs, unless they were adequately informed, or should otherwise have had reason to know, that the material was infringing or illegal. Immunity would be conditional upon the archival organisations being able to demonstrate appropriate risk assessment practices including, as appropriate, the use of suitable metadata or digital object tagging systems to enable the identification of high-risk content – **limited liability for accessioning digital objects.**
- Provision of access to digital objects deposited with or harvested by authorised archives and repositories would remain subject to:
    - limits upon the purposes for which the deposited material could be used e.g. where required by copyright law, data protection law or other statutory requirement;

169 *Ibid*

170 *Ibid*

- controls on the time at which readers could first use the material e.g. by existing statutory requirement, or where embargoes are agreed with depositors;
- controls on the type of readers who could use the material e.g. researchers;
- controls on number of readers who could use the material at any one time – **precise limits on the access to and reuse of accessioned digital objects.**

- Embargoed digital objects deposited with, or harvested by, authorised repositories would be exempt from the Freedom of Information Act 2000, except where their disclosure would be in the substantial public interest – **clear protection for embargoed digital objects and a clear rule for access under statute.**
- Immunity could be granted to authorised archives and repositories from liability for copyright infringement, or any other content liability, in materials contained in PDArcs which were made available to third parties, unless the archival organisations were adequately informed, or should otherwise have had reason to know, that the material was infringing or illegal. Immunity would be conditional upon the repositories being able to demonstrate appropriate risk assessment practices including, as appropriate, the use of suitable metadata or digital object tagging systems to enable the identification of high-risk content – **limited liability for providing access to digital objects.**

5. Conclusions and Recommendations

> *"It is only slightly facetious to say that digital information lasts forever - or five years, whichever comes first"* ***Jeff Rothenberg*****, RAND Corporation**[171]

5.1 Starving at a Feast?

It's something of a paradox. At a time when private individuals have the greatest opportunity to create, collect and broadcast personal content - to record their digital lives - the fear is that, despite capacious storage, despite technological innovation, and despite the ever so human desire to leave some record of our passing behind, the digital archives we bequeath to the future researcher may be less valuable sources of information about our lives than we would have hoped. To some degree it is the curse of all new technologies: often moving faster than our comprehension of their importance, they write and having writ move on, leaving us to contemplate the things we might have preserved, had we recognised their importance and understood their inherent ephemerality.

There are numerous reasons why we may fail to capture a full picture of this explosive period of personal creation. Despite our increased capacity, there will likely be too much to store: despite our interactivity valuable information will fail to get caught in the net. And ultimately, unless it is possible to store everything, choices have to be made about what is saved and what is not, and our captured priorities and preferences may not endear us to future researchers. The limits of technology, and of futurology, may of necessity bound our actions in preserving valuable digital content: the key questions this research paper addresses are whether we should simply assume the law will do the same; or, if we are to suggest that it should not, or need not, be an obstacle, how we can work with it, or actively utilise it, to achieve our goals.

In many respects, the laws relating to personal digital archives (PDArcs) are no different from those relating to paper archives – who owns the copyrights? whose privacy or confidences are at issue? how and when should we have access to materials? are there things that should not be archived, or that should not be made readily publicly accessible? The important differences actually lie, not in the letter of the law, but rather in how the spirit of the law is going to be interpreted by archivists, researchers, the public and the courts in the light of contemporaneous social developments, such as online social networking and sharing of user generated content. These social developments blur

171 Rothenberg, J. (1995) Ensuring the Longevity of Digital Documents. *Scientific American*, 272(1): 42-47

the normative boundaries in and on which legal interpretation is grounded. If the conditions are right, they can lead to the encouragement of new ways of thinking about how existing laws might be harnessed to new ends, as with the Creative Commons, or how they could be reformed to more readily reflect contemporary social requirements, as is slowly taking place with legal deposit.

Concerns about legal issues often arise from the assumption that the role of archives and repositories is implicitly one of direct responsibility for, and 'top-down' control over, such issues. An important lesson from Web 2.0 technologies, like Wikipedia and Digg, is that there may be significant gains to be obtained from disaggregating not just content ownership, but also control, in digital resources. The role of the repository in preserving PDArcs need not be solely, or simply, a 'gatekeeper' role, it may in some circumstances more usefully act as a guide, a facilitator, or a broker. In terms of the law, that may translate to providing guidance to those creating PDArcs on how to structure, or tag, or add metadata to their PDArc so that repositories can reduce the time spent on legal oversight during accession. It might mean developing, or advising on the development of, software tools which aid in the construction/aggregation of PDArcs from digital content hosted in a variety of commercial services. It could involve working with commercial services and users on ways to allow the harvesting of digital content for archiving and future research, that provide benefits to all parties – competitive advantage to the commercial services, preservation of personal digital content for users, and access to personal digital content under pre-agreed conditions for a repository.

Archivists have already embraced new technologies for capturing digital content. When dealing with the legal ramifications of PDArcs, they will need to consider new ways of interacting with depositors, new alliances with public and private organisations, new mechanisms/methods for achieving legal compliance, and, initially at least, to tolerate what may come as a slightly disconcerting voyage outside their legal comfort zone.

5.2 Ways Forward

This research paper has provided an overview of the legal and ethical questions arising from the collection, preservation and ultimate release to researchers/the public of personal digital archives. This overview underpins the series of recommendations set out below.

Recommendation 1 – Pragmatism

Archivists should adopt a pragmatic approach to the legal risks inherent in the collection and preservation of personal digital archives.

While there are undoubtedly legal risks associated with the collection, preservation and ultimate release to researchers/the public of personal digital archives, such risk is generally low level, and effective protection can be obtained via the type of risk assessment and risk management strategies outlined above. No system of risk management can totally remove the threat of legal action, nor is it practical to attempt to achieve this. Effective risk management practices can, however, reduce the likelihood of such action and, more importantly, significantly reduce the negative effects (reputationally and financially) arising from successful legal challenges. It is important for repositories to consider the reasonableness of adopting, or not adopting, particular risk amelioration strategies in the context of particular types of PDArc, and particular types of use, and in the light of contemporary sectoral practices and understandings. Provision of adequate and appropriately pitched information to depositors, repository staff and end-users, can build common understandings, and prevent disputes arising from misinterpretations of repository practices. Establishing a grievance procedure is an effective way of bringing disputes to settlement via mediation. Many injured third parties will be effectively assuaged by the fact that their complaint is being treated through a formal procedure. Lessons in this area can be learnt from data collection/harvesting practices across the digital environment, from the Internet Archive, to Google StreetView and Google Books.

Recommendation 2 – Risk Assessment and Policy Frameworks

Archives seeking to accession personal digital archives should have a flexible legal policy framework, based on an initial background and risk assessment, which contains clear and documented processes for deposit and access management, policy and process audit and risk amelioration, and which incorporates the ability to effect coherent change management in the light of shifts in environmental factors.

For risk assessment and risk management strategies to be effective, both in terms of providing protection against legal risk, and in terms of depositor and user confidence, they have to be used in practice and be seen to be used. The legal risk assessment should seek to identify the legal risks involved in the use of particular technologies, tools and collection methodologies; and, if carried out early enough, can help to influence those choices. It may also examine, as appropriate, options for effective compliance with particular legal obligations; and effective administration of information gathering tools and practices, e.g. ensuring the legal risks are understood by depositors, repository staff and end-users, that legal liability for content is appropriately allocated and explained, and that there are adequate processes in place to limit researcher and research subject exposure to liability.

A legal policy framework should at a minimum contain formal publicised positions on the key legal issues faced by the repository, supported by such guidance documentation, documented processes, staff training, and allocation of internal staff responsibilities as are necessary. Maintenance of the legal policy framework should be an ever-greening process with constant review of its rationales, permitting the updating of its elements to best achieve the aims of the repository. As such, the legal risk assessment should not be treated as a start of project 'box ticking' exercise, but rather as a mechanism underpinning an efficient management process. Changes to repository goals, methodology, online tools etc. will require a fresh assessment of the legal risks. Repository staff should document any legal issues encountered, whether these were anticipated in the risk assessment, and how they were handled. A strategy of encouraging repositories to discuss good practice in the practical handling of legal risks in the online environment will be an essential part of ingraining effective legal compliance processes into a rapidly developing field.

Recommendation 3 – Development of Tools and Standards

Archivists have a vital role to play in encouraging the provision and adoption of tools and standards by commercial organisations, and the adoption of those tools by the public, which will simplify the process of collection and preservation of personal digital archives - this issue will require further consideration.

The concept of the PDArc is still very much in a developmental phase, with commercial entities looking for innovative ways to utilise the data collected by users, on personal computer equipment as well as in Web 2.0 services and other online environments, to offer new services or tools. Archivists thus have a golden opportunity to leverage the success of existing repositories, e.g. those used by amateur genealogists, by demonstrating the value to end-users, and simultaneously to commercial bodies, of obtaining tools for, and standardising aspects of, the creation of PDArcs to make them more accessible to future generations.

Recommendation 4 – Strategic Partnerships

There are potential synergies in developing strategic partnerships between archives/ repositories and commercial providers of services, such as social networking services, in order to capture/ harvest digital content for archiving and future research, these should be explored.

There have already been some successful commercial/non-profit collaborations in online archiving, of which the Alexa Internet/Internet Archive relationship is probably the largest scale example. High profile repositories, such as the British Library, have valuable brand recognition that could be used in conjunction with commercial services to promote the archiving and preservation of 'digital public' PDArcs on a large scale. Collection/harvesting and preservation of PDArcs could take place

with user deposit agreements made available to would-be depositors by the commercial services on behalf of a repository, and using PDArc tools/standards designed in collaboration between the commercial service and the repository. The repository would thus gain access to a supply of PDArcs, the public would gain the opportunity to preserve their PDArc for posterity, and the commercial service would gain access to a valuable brand and could use archiving as a selling point. Clearly, the detail of such collaboration would need to be considered carefully, notably with regard to the level of commitment that the repository would be making to long-term retention and preservation of 'digital public' PDArcs; and the liability of the repository with regard to accidental loss or destruction of deposited digital materials. This could be limited via the deposit agreement in a similar fashion that end-user licence agreements (EULAs) limit the liability of computer software manufacturers with regard to failure of software. Equally the repository/commercial provider could provide a tiered archiving and preservation service, contingent upon an initial fee or a maintenance fee, and accepting greater liability.

Recommendation 5 – Information and Education in Context

If there is to be wider public interactivity with the formal archival process for personal digital archives, then archivists need to consider how they deliver appropriate information about deposit and access policies, deposit agreements and metadata, pitched at the right level, to the right audience

If repositories are going to move away from bespoke, or limited use, deposit agreements (and any move towards large scale collection of 'digital public' PDArcs, will inevitably mean such a move) then they will need to think carefully about the type of deposit framework they wish to create, from in-house policy guidance, through metadata schemas, to the deposit agreements and explanatory material. Ideally, all of these aspects should combine to form a coherent whole, so that deposit policy is clear to repository staff (who may need to explain it to depositors, regulators and courts), depositors, and interested/affected third parties. 'Layered' deposit agreements and deposit policy documents may permit the same set of documentation to be used across a wide range of parties, thus reducing costs and providing information at a comprehension level that the party concerned requires. Both the Creative Commons and some Information Commissioners use 'layered' documentation to provide various types of information about the same subject to different audiences, from the layperson to legal experts.

Recommendation 6 – Encouraging flexibility in legal protections and freedoms

There are important lessons to be learned from the Creative Commons approach to copyright that are applicable to other legal issues facing archivists

Layered licences are not the only lesson that can be learned from the Creative Commons. Equally important is the use of easily recognisable icons to indicate particular licence conditions, e.g.

List 1 – Examples of Creative Commons icons[172]

This license lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation.

This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms.

This license is the most restrictive of our six main licenses, allowing redistribution. This license is often called the 'free advertising' license because it allows others to download your works and share them with others as long as they mention you and link back to you, but they can't change them in any way or use them commercially.

172 Creative Commons – Licenses
http://creativecommons.org/about/licenses/

However, if an icon-based approach is to be successfully adopted, it will be important to try to avoid 'icon proliferation', particularly between similar repositories, e.g. deposit libraries. The value of the Creative Commons icon set is that it is immediately recognisable to depositors and potential re-users wherever they are. In the digital learning environment, other repository organisations have adopted their own icon sets for similar purposes, e.g. It is suggested that this approach, of each repository creating its own icons, often duplicating the function of other organisations' icons, should be deprecated.

List 2 - Examples of AEShareNet icons[173]

May be freely used and copied for educational purposes but the owner retains full control of its use for any other purposes.

Material may be used and enhanced by anyone free of charge but copyright in published enhancements consolidates with the original owner.

The material may be freely copied but only in its original form including the owner's copyright notice.

Recommendation 7 - Publicity and Authority

Archivists must be more proactive about promoting the possibilities of their PDArc-related work to the 'digital public', and in demonstrating that their legal and ethical practices can allow them to achieve important social ends with little risk to the individual.

There is currently considerable interest amongst the public in personal histories, particularly, as already noted, in relation to genealogical studies/research. In combination with the rise of online social networking services and tools, this is potentially a defining moment for the future development of PDArc collection, preservation and re-use, in the sense of repositories being able to influence and embed understandings of the value of their archival work in popular culture. Future trends in public opinion may not be so positive, notably the possibility of public backlashes against perceived privacy invasions by social networking services, the State, and commercial interests. Archivists could have an important role to play in establishing an acceptable set of ground rules, both legal and ethical, for collection, preservation and re-use, which take into account the rights and wishes of depositors, as well as the interest of third parties.

Recommendation 8 - Standardisation

Archivists and their umbrella organisations should consider developing and implementing, as far as possible, standardised deposit and access policies, deposit agreements and metadata standards for personal digital archive collections to aid interoperability.

As noted above, in Recommendation 6, the value of preserved PDArcs can be increased by enabling interoperability between repositories, i.e. where repositories adhere to the same deposit and access policies, deposit agreements and metadata standards for PDArcs, it should be possible for repositories to legitimately exchange preserved PDArcs (if one repository has a collection for which a PDArc is more appropriate), or hand over control of them should this become necessary (e.g. if a repository closes or loses funding) or permit interoperable network access to them. This will require co-ordinated action between repositories or networks of repositories to ensure that standardisation can be achieved. Lessons can be learned from the interoperability experiences of organisations such as the EU-funded Digital Repository Infrastructure Vision for European Research

---

173 AESharenet - Licensing
http://www.aesharenet.com.au/coreBusiness/

(DRIVER)[174] – "One important semiformal aspect to DRIVER's working is mentoring – linking those running newly established repositories with those with more practical experience."[175]

Recommendation 9 – Legislative Action

Archivists and their umbrella organisations should lobby the government, and in particular the Department for Culture, Media and Sport, for an improved system of legal deposit for all digital objects made available to the public (as per s.12(5), s.13A(2) & s.13B(6) CDPA 1988), which provides archives with a clearly defined system of limited liability for accessioning and providing access to those digital objects, covering the major areas of legal risk, and subject to institutional provision of appropriate risk assessment and risk management strategies, and appropriate ethical guidelines and practices.

While obtaining a change in the law is often a long-winded affair, legislative reform could potentially cut through the Gordian knot of legal risks that face repositories, and provide a clearly defined system of limited liability for accessioning and providing access to all digital objects. However, pressure on Parliamentary time means that issues that are not brought firmly to the attention of legislators or regulators acting under legislation, are likely to languish. While this research paper has suggested a number of methods of working more effectively within the existing regime, pressure should still be maintained on government, and on bodies such as the Legal Deposit Advisory Panel, to make appropriate changes to the law, or enabling regulations under existing law.

Recommendation 10 – Delegation of Deposit Powers

Legal Deposit libraries should be permitted to delegate their archiving powers in certain areas to other 'authorised' organisations, including smaller archives and libraries, to collect, archive and make available digital objects. Authorisation should be conditional upon the organisation in question demonstrating that they have appropriate risk assessment and risk management strategies and appropriate ethical guidelines and practices. Organisations should be subject to regular audit on these issues, by the authorising body.

This research paper has suggested that the system of legal deposit needs a thorough and wide-ranging overhaul. The current system is premised on a 'publishing' environment that has been comprehensively overtaken by both technological advances and social change. In the new highly-paced environment, the idea of leaving the preservation of highly diverse digital materials, such as PDArcs, solely to the official Legal Deposit Libraries makes little sense. Some degree of subsidiarity of legal deposit is required - matters ought to be handled at the level of the most competent organisation (e.g. regional repositories or subject specific repositories), and central authority/ies (the Legal Deposit Libraries) should have a subsidiary function, performing only those tasks which cannot be performed effectively at a more immediate or local level. Such a role might include a number of elements of Recommendations 2- 9, e.g. where a central authority or central authorities can most effectively play a role in setting standards, negotiating with the private sector, and promoting legal and ethical practices.

---

174 Digital Repository Infrastructure Vision for European Research (DRIVER) http://www.driver-support.eu/index.html

175 Charlesworth *et al* (2008) *Feasibility study into approaches to improve the consistency with which repositories share material*, n.154

Acknowledgements

Very many thanks to participants of two focus group meetings for Legal and Ethical Issues held at the British Library Conference Centre in June 2008: Guy Baxter, Victoria & Albert Museum; Else Churchill, Society of Genealogists; Maxine Clarke, Nature Publishing Group; Frances Harris, British Library; Arwel Jones, National Library of Wales; Jack Latimer, Community Sites; Hannah Little, HATII, University of Glasgow; Luke McKernan, British Library; Kathleen O'Riordan, Media & Film, University of Sussex; Helene Snee, University of Manchester; Tilli Tansey, Wellcome Trust Centre for the History of Medicine; Susan Thomas, Bodleian Library, University of Oxford; Dave Thompson, Wellcome Library; Lynn Young, British Library.

Special thanks to members of the Digital Lives project: Jamie Andrews, Neil Beagrie, Katrina Dean, Alison Hill, Jeremy Leighton John, Rory McLeod, David Nicholas, Robert Perks, Ian Rowlands, John Tuck, Paul Wheatley and Peter Williams.

Bibliography

Books

Akdeniz, Y. (2008) *Internet Child Pornography and the Law: National and International Responses*. Ashgate.

Bailey, S. & Taylor, N. (2009) *Civil Liberties Cases, Materials, and Commentary* (6th ed.). Oxford University Press.

Behrnd-Klodt, M.L & Wosh, P.J. (eds.) (2005) *Privacy & Confidentiality Perspectives: Archivists & Archival Records*. Society of American Archivists.

Behrnd-Klodt, M.L (2008). *Navigating Legal Issues in Archives*. Society of American Archivists.

Calvert, C. (2000) *Voyeur Nation: Media, Privacy, and Peering in Modern Culture*. Westview Press.

Carey, P. (2009) *Data Protection: A Practical Guide to UK and EU Law*. (3rd ed.). Oxford University Press.

Collins, M. (2005) *The Law of Defamation and the Internet* (2nd ed.). Oxford University Press.

HM Treasury (2006) *Gowers Review of Intellectual Property*. HMSO.

Jay, R. & Hamilton, A. (2007) *Data Protection Law and Practice* (3rd ed.). Sweet & Maxwell.

Kenyon, A. (2006) *Defamation: Comparative Law and Practice*. UCL Press.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. Basic Books.

Miller, C. J. (2000) *Contempt of Court* (3rd ed.). Oxford University Press.

Padfield, T. (2007) *Copyright for Records Managers and Archivists* (3rd ed.). Facet Publishing.

Pedley, P. (2007) *Digital Copyright* (2nd ed.). Facet Publishing.

Stead, A. (2008) *Information Rights in Practice: the non-legal professional's guide*. Facet Publishing.

Articles & Chapters

Beagrie, N. (2005) Plenty of Room at the Bottom? Personal Digital Libraries and Collections. *D-Lib Magazine* 11 (6).
http://www.dlib.org/dlib/june05/beagrie/06beagrie.html

Besek, J.M Coates, J. Fitzgerald, B. Mossink, W. LeFurgy, W.G. Muir, A. Rasenberger, M. Weston, C.D. (2008) Digital Preservation and Copyright: An International Study. *International Journal of Digital Curation* 3(2): 103-111.
http://www.ijdc.net/index.php/ijdc/article/viewFile/90/61

Charlesworth, A. (2000) Clash of the Data Titans: US and EU Data Privacy Regulation. *European Public Law* 6: 253-274.

Charlesworth, A. (2006) The future of UK data protection regulation. *Information Security Technical Report* 11(1): 46-54.

Churchill, E. & Ubois, J. (2008) Designing for digital archives. *Interactions* 15(2): 10-13.

Darlington, J. Finney, A. & Pearce, A. (2003) Domesday Redux: The rescue of the BBC Domesday Project videodiscs. *Ariadne* 36.
http://www.ariadne.ac.uk/issue36/tna/

Field, C. (2004) Securing digital legal deposit in the UK: the Legal Deposit Libraries Act 2003. *Alexandria* 16 (2): 87-111.

Gemmell, J. Bell, G & Lueder, R. (2006) MyLifeBits: a personal database for everything. *Communications of the ACM* 49(1): 88-95.

Gibby, R. & Green, A. (2008) Electronic Legal Deposit in the United Kingdom. *New Review of Academic Librarianship*. 14 (1 & 2): 55-70.

Goldstone R. & Gill, J. Web Site Operators & Liability for UGC - Facing up to Reality? *Society for Computers & Law*, 31 Dec 2008.
http://www.scl.org/site.aspx?i=ed9981

Gross, R., Acquisti, A. & H. John Heinz, I. (2005) Information revelation and privacy in online social networks. In: *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*, pp 71-80. ACM.

Hinduja, S. & Patchin, J. W. (2008) Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence* 31(1): 125-146.

Jacobsen, G. (2008) Web Archiving: Issues and Problems in Collection Building and Access. *Liber Quarterly* 18 (3/4).
http://liber.library.uu.nl/publish/issues/2008-3_4/index.html?000273

Joint, N. (2006) Risk assessment and copyright in digital libraries. *Library Review* 55(9): 545 – 548.

Korn, N., Oppenheim, C. (2006) Creative Commons licences in higher and further education: Do we care? *Ariadne* 49.
http://www.ariadne.ac.uk/issue49/korn-oppenheim/

Lenthall, E. & Harman-Wilson, R. (2008) The Web of Contempt: A trap for website operators? *Computer Law & Security Report* 24(6): 568-570.

Marshall, C. (2006) *Maintaining Personal Information: Issues Associated with Long Term Storage Preservation and Access*.
http://www.csdl.tamu.edu/~marshall/PIM%20Chapter-Marshall.pdf

Mearian, L. (2009) Internet Archive to unveil massive Wayback Machine data center. *Computerworld*, 19 March. http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=hardware&articleId=9130081&taxonomyId=12&intsrc=kc_top

Mercado-Kierkegaard, S. (2006) Blogs, lies and the doocing: The next hotbed of litigation? *Computer Law & Security Report* 22(2): 127-136.

Milne, R. & Tuck, J. (2008) Implementing e-Legal Deposit: A British Library Perspective. *Ariadne* 57.
http://www.ariadne.ac.uk/issue57/milne-tuck/

Moreno, M. A., Fost, N. C. & Christakis, D. A. (2008) Research Ethics in the MySpace Era. *Pediatrics* 121(1): 157-161.

Nijhawan, D. R. (2003) The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States. *Vanderbilt Law Review* 56(3): 939-976.

Nissenbaum, H. (2004) Privacy as Contextual Integrity. *Washington Law Review* 79(1): 119-158.

Parry, O., Mauthner, N.S. (2004) Whose data are they anyway? Practical, legal, and ethical issues in archiving qualitative research data. *Sociology* 38(1): 139-52.

Petley, J. (1996) Savoy scrapbook. *Index on Censorship*, 25(1): 162-166.

Phillips, J. (1989) Copyright in Spoken Words - Some Potential Problems. *European Intellectual Property Review* (No.7): 231-234.

Procter, M. (2006) The end of [local] history: will twenty-first century sources survive? *Local Historian* 36(4): 238-253.

Rothenberg, J. (1995) Ensuring the Longevity of Digital Documents. *Scientific American* 272(1): 42-47.

Shepherd, E. (2007) Freedom of Information and Records Management in the UK: What has been the Impact? *Journal of the Society of Archivists* 28(2): 125-138.

Shepherd, E. & Ennion E. (2007) How has the implementation of the UK Freedom of Information Act 2000 affected archives and records management services? *Records Management Journal* 17(1): 32-51.

Tuck, J. (2008) Web Archiving in the UK: Cooperation, Legislation and Regulation. *Liber Quarterly* 18 (3/4).
http://liber.library.uu.nl/publish/issues/2008-3_4/index.html?000258

Wacks, Raymond. (2006) Why There Will Never Be an English Common Law Privacy Tort. In: *New Dimensions in Privacy Law*, edited by A. T. Kenyon and M. Richardson, pp 154-183. Cambridge University Press.

Williams, P. Dean, K. Rowlands, I. & John, J.L. (2008) Digital Lives: Report of Interviews with the Creators of Personal Digital Collections. *Ariadne* 55.
http://www.ariadne.ac.uk/issue55/williams-et-al/

Reports

Besek, J.M *et al* (2008) *International Study on the Impact of Copyright Law on Digital Preservation*. Joint report of The Library of Congress National Digital Information Infrastructure and Preservation Program; The Joint Information Systems Committee; The Open Access to Knowledge (OAK) Law Project; and The SURF foundation.
http://www.digitalpreservation.gov/library/resources/pubs/docs/digital_preservation_final_report2008.pdf

Beunen, Annemarie & Schiphof, Tjeerd, (2006) *Legal aspects of web archiving from a Dutch perspective*. Report commissioned by the Dutch National Library. http://www.kb.nl/hrd/dd/dd_projecten/webarchivering/documenten/KB_Legal_Aspects_WebArchiving_EN.pdf

CEDARS Project (2002) *CEDARS Guide to Intellectual Property Rights*.
http://www.leeds.ac.uk/cedars/guideto/ipr/guidetoipr.pdf

Charlesworth, A. (2003) *Legal Issues relating to the archiving of internet resources in the UK, EU, USA and Australia*, a study undertaken for the JISC and Wellcome Trust.
http://www.jisc.ac.uk/uploaded_documents/archiving_legal.pdf

Charlesworth, A. Ferguson, N. Massart, D. Van Assche, F. Mason J. Radford, A. Smith, N. Tice, R. Collett, M. Schmoller, S. (2008) *Development of Good Practice Guidelines for Repository Owners*, Project Report, BECTA, 14 February 2008.

Charlesworth, A. Ferguson, N. Morgan, E.L. Schmoller, S. Smith, N. & Zeitlyn, D. (2008) *Feasibility study into approaches to improve the consistency with which repositories share material*. Project Report, JISC, 5 November 2008.
http://ie-repository.jisc.ac.uk/256/1/jisc-clax-final-report-repocon.pdf

Department of Culture, Media and Sport (2003) *The Government's Response to the Fifth Report of the Culture, Media and Sport Select Committee on 'Privacy and Media Intrusion'* (HC 458) Session 2002-2003, Cm 5985, October 2003, TSO.
http://www.culture.gov.uk/images/publications/895260Cm5985PRIVACY710.pdf

OECD. (2007) *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking*.
http://213.253.134.43/oecd/pdfs/browseit/9307031E.PDF

Rothenberg, J. (1999) *Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation*. A Report to the Council on Library and Information Resources.
http://eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/17/3d/34.pdf

Other

Digital Curation Centre (2005) Briefing Paper: Freedom of Information (McGinley, M.)
http://www.dcc.ac.uk/resource/briefing-papers/freedom-of-information/

Digital Curation Centre (2007) Briefing Paper: Data Protection (Anon.)
http://www.dcc.ac.uk/resource/briefing-papers/data-protection.pdf

Center for Information Policy Leadership (2007), *Ten steps to develop a multilayered privacy notice*.
http://www.hunton.com/files/tbl_s47details%5Cfileupload265%5C1405%5Cten_steps_whitepaper.pdf

ICO (2007) Freedom of Information Act Awareness Guidance No. 12: When is information caught by the Freedom of Information Act? Version 2.0 5.
http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_12_info_caught_by_foi_act.pdf

Lord Chancellor's Code of Practice on the discharge of public authorities functions under Part I of the Freedom of Information Act 2000 (2004).
http://www.justice.gov.uk/guidance/docs/foi-section45-code-of-practice.pdf

Lord Chancellor's Code of Practice on the Management of Records (2002).
http://www.foi.gov.uk/codemanrec.pdf

National Archives (undated) *The National Archives Publication Scheme: Copyright and the publication scheme*.
http://www.nationalarchives.gov.uk/foi/pubschemes.htm

National Archives (2000) *Data Protection Act 1998: A Guide for Records Managers and Archivists*, Public Record Office.
http://www.nationalarchives.gov.uk/documents/dpguide.pdf

National Archives, Society of Archivists, Records Management Society & National Association for Information Management (2007) *Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998*, The National Archives.
http://www.nationalarchives.gov.uk/documents/dp-code-of-practice.pdf

National Archives (2008) *Data Protection Policy Statement*.

http://www.nationalarchives.gov.uk/legal/pdf/policy-feb08.pdf

National Archives (2008) *Procedures for handling personal information under the Data Protection Act 1998.* http://www.nationalarchives.gov.uk/legal/pdf/procedures-feb08.pdf

Office of Public Sector Information (2008) *Copyright Guidance: Freedom of Information Publication Schemes.* http://www.opsi.gov.uk/advice/crown-copyright/copyright-guidance/freedom-of-information-publication-schemes

Useful Resources

The Creative Commons
http://creativecommons.org/

Creative Commons, License Your Work
http://creativecommons.org/about/license/

The Internet Archive
http://www.archive.org/about/about.php

Internet Watch Foundation
http://www.iwf.org.uk/

The Personal Archives Accessible in Digital Media (paradigm) project
http://www.paradigm.ac.uk/index.html

The UK Web Archiving Consortium (UKWAC)
http://www.webarchive.org.uk/

Legislation

NB: UK Acts listed in this section are cited to their originally published form, unless otherwise indicated. To view consequent amendments to UK Acts, please consult the UK Statute Law Database at: http://www.statutelaw.gov.uk/

Council of Europe, Draft Recommendation: A European Policy on access to archives
https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2000)93&Sector=secCM&Language=lanEnglish&Ver

EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF

British Library Act 1972
http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1972/cukpga_19720054_en_1

Copyright, Designs and Patents Act 1988 (unofficial consolidated version)
http://www.ipo.gov.uk/cdpact1988.pdf

Contempt of Court Act 1981
Available via http://www.statutelaw.gov.uk/

Criminal Justice Act 1988
http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880033_en_1.htm

Criminal Justice and Immigration Act 2008
http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1

Criminal Justice and Public Order Act 1994
http://www.opsi.gov.uk/acts/acts1994/ukpga_19940033_en_1

Defamation Act 1996
http://www.opsi.gov.uk/Acts/acts1996/ukpga_19960031_en_1

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Data Protection (Processing of Sensitive Personal Data) Order 2000
http://www.opsi.gov.uk/si/si2000/20000417.htm

Electronic Commerce (EC Directive) Regulations 2002
http://www.opsi.gov.uk/si/si2002/20022013.htm

Freedom of Information Act 2000 (England & Wales)
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1

Legal Deposit Act 2003
http://www.opsi.gov.uk/acts/acts2003/ukpga_20030028_en_1

Obscene Publications Act 1959
Available via http://www.statutelaw.gov.uk/

Obscene Publications Act 1964
Available via http://www.statutelaw.gov.uk/

Protection of Children Act 1978
Available via http://www.statutelaw.gov.uk/

All hyperlinks checked 7 October 2009

Annex A – Interview/Focus Group Schedules

The following interview/focus group schedules were prepared as part of the preliminary work. They were not used for interviews during this phase of *digital lives*, but were used as the basis for two focus group meetings at the British Library on 24 June 2008. Input from the two focus groups was fed into the writing of this report.

PDArcs - Repositories - Interview Schedule

No.	Section 1 - Accession of Digital Material	Follow-ups	Pathway
1	What are the key legal/ethical issues that you consider when receiving digital material from private individuals?	What types of digital material do you most commonly receive on deposit? Do you treat digital material differently in legal terms than non-digital material?	Go to Q.2
2	Is digital material received on deposit from private individuals generally made available to the public, usually only made available to particular groups of user (e.g. academics), or otherwise subject to particular conditions of use/access?	What types of conditions, if any, are most commonly attached to deposits of personal digital archives by private individuals?	Go to Q.3
3	Have you refused deposit of a personal digital archive by a private individual due to restrictive conditions being imposed on its access and use?	Do personal digital archives with restrictive conditions on access and use (e.g. 'dark' archives)pose significant questions of cost/benefit to your repository, or are such conditions simply accepted as a long-term cost of obtaining material?	Go to Q.4
4	Has a user (or other 3rd party - police, government etc.) ever sought to overturn a decision to deny access, or a depositor's request to deny access to digital material deposited by private individuals?	Was this an 'internal appeal' within the repository, a request to the original donor, a request to a third party with interests in the archived material, or a legal appeal?	Go to Q.5
5	Have you ever had a request for digital material deposited by private individuals under the Freedom of Information legislation, or via other legal routes?	If you have received an FOIA request, how did you deal with it?	Go to Q.6
6	Have you ever sought legal advice on the issues pertaining to deposit of digital material accessioned by repositories from private individuals?	On which issues? Did you obtain useful/ accurate answers to your questions? Did you change internal policy or documentation as a result of those answers?	Go to Q.7
7	Are there particular interest groups/forums/ or other sources of community information that those running archives and repositories can draw upon for information on digital archiving?	Are any of these sources of community information regarded as particularly important resources? Have you used any of these sources of community information? Did you find them useful in addressing your issues?	Go to Q.8

No.	Section 2 - Deposit and Deposit Agreements	Follow-ups	Pathway
8	Do you require depositors to sign a deposit agreement before supplying material to your archive or repository?	Does that deposit agreement impose different terms for digital/non-digital materials?	If YES go to Q.9 If NO go to Q.12
9	Do you provide guidance on the legal and ethical conditions your deposit agreement contains?	How detailed is that guidance, and why? Does your deposit agreement impose warranties and /or indemnities on depositors? Are your staff in a position to discuss legal/ethical conditions in deposit agreements with would-be depositors?	Go to Q.10
10	Do you believe that the average depositor understands the legal/ethical implications of conditions contained in such deposit agreements?	On what evidence do you base that belief?	Go to Q.11
11	Can depositors easily negotiate the conditions under which you accept digital materials?	What process do such negotiations follow? With whom do the negotiations take place?	Go to Q.12
12	Do you accept electronic deposit of digital materials?	Does electronic deposit permit the same degree of flexibility in negotiation of deposit conditions as your off -line deposit process?	Go to Q.13

No.	Section 3 - Re-use of Archive Material and User Agreements	Follow-ups	Pathway
13	Do you require users to sign a user agreement before accessing material in your archive or repository?	Does that user agreement impose different terms for digital/non-digital materials?	Go to Q.14
14	Do you provide users with explicit guidance on appropriate use and re-use of archive material?	Are your staff in a position to discuss legal/ethical conditions in the user agreement with users? Are there any other sources (e.g. professional bodies, funding bodies) that provide useful information? Are there particular examples of good practice you would recommend?	Go to Q.15
15	Do you believe that the average depositor understands the legal/ethical implications of conditions contained in such deposit agreements?	On what evidence do you base that belief?	Go to Q.16
16	Have you refused access to a personal digital archive in your collection on the ground that the proposed use/re-use would raise legal/ethical issues not envisaged by the depositor?	What legal/ethical-based justifications for denying access to archival material might there be?	Go to Q.17
17	In your experience, when using digital material received by your archive/repository from private individuals, do users follow the relevant conditions for its use strictly?	If you think users don't always follow the conditions for its use strictly, in what circumstances would you consider them to be most likely to not follow them?	Go to Q.18
18	Are you aware of the use of any digital material, received by your archive/repository from private individuals, which has resulted in complaints either by the depositor or by third parties?	Did the conditions for the digital material's use clearly cover the circumstances about which the complaints were made? Were the complaints upheld? If so, what were the consequences? If not, why not?	Go to Q.19

No.	Section 4 - Metadata	Follow-ups	Pathway
19	Does your archive/repository support legal metadata for issues such as copyright ownership and licensing information, or data protection status?	How commonplace is legally-oriented metadata in digital repositories?	If YES go to Q.20 If NO go to Q.22
20	Do you find that digital material received by your archive/repository from private individuals currently comes with adequate metadata to enable effective and efficient use of the material?	Is digital material more or less likely to have useful metadata than non-digital material?	Go to Q.21
21	Do you provide guidance to would-be depositors on how to add metadata to their digital archives?	Are there any other sources (e.g. professional bodies, funding bodies) that provide useful information? Are there particular examples of good practice you would recommend?	Go to Q.22
22	Do you think that the publicity surrounding data protection and copyright issues on the internet has had an influence on the way in which the use and reuse of digital material in repositories is treated?	Do you think that depositors of material in digital repositories are more or less likely to assert intellectual property rights (e.g. copyright) in their deposited materials, than depositors of non-digital materials?	Go to Q.23

No.	Section 5 - Adding Value to Archive Material	Follow-ups	Pathway
23	How do you think that repositories could most effectively improve the usefulness of digital material provided by private individuals?	Is more metadata a solution? Who should provide the metadata, the depositor or the repository? Is there an appropriate standard for metadata for material of this type?	Go to Q.24
24	Would some form of symbolic representation indicating appropriate use of digital material be helpful?	Would a model like that of the Creative Commons symbols be helpful in speeding up decisions about the use of digital material provided by private individuals?	Go to Q.25
25	If you could change one thing about the law relating to your work in archives/repositories, what would it be?		END

PDArcs – Repositories – Interview Schedule background

No.	Section 1 – Accessing Archive Material	Rationale	Pathway
1	What are the key legal/ethical issues that you consider when receiving digital material from private individuals?	This aims to identify those legal/ethical issues most important to archives/repositories. This may vary depending on the type of digital material to be used, but there are likely to be common themes to explore.	Go to Q.2
2	Is digital material received on deposit from private individuals generally made available to the public, usually only made available to particular groups of user (e.g. academics), or otherwise subject to particular conditions of use/access?	The degree of control exercised over access to digital materials will influence the degree of control of use and reuse that is then exercised by finer legal tools, such as © and privacy laws. This aims to assess the extent to which 'gross access control' is preferred to 'fine use control'.	Go to Q.3
3	Have you refused deposit of a personal digital archive by a private individual due to restrictive conditions being imposed on its access and use?	Archives/repositories may be disinclined to accept personal digital archives with restrictive conditions (e.g. long-term 'dark archives). This aims to assess whether material may be lost due to overly restrictive conditions – it may be necessary to provide explanation and guidance to depositors on this point.	Go to Q.4
4	Has a user (or other 3rd party – police, government etc.) ever sought to overturn a decision to deny access, or a depositor's request to deny access to digital material deposited by private individuals?	Oversight of decisions about access to digital materials will be key to ensuring consistency in repository/user community practice.	Go to Q.5
5	Have you ever had a request for digital material deposited by private individuals under the Freedom of Information legislation, or via other legal routes?	Some repositories (part of or attached to 'public authorities', as defined by FOIA) may have a legal obligation to disclose information provided by private individuals. It is unclear how common this practice currently is, or the impact on repository practices.	Go to Q.6
6	Have you ever sought legal advice on the issues pertaining to deposit of digital material accessioned by repositories from private individuals?	It would be useful to build up a knowledge base derived from expert advice sought by repositories – it would also be useful to identify inconsistencies in such advice.	Go to Q.7
7	Are there particular interest groups/forums/ or other sources of community information that those running archives and repositories can draw upon for information on legal issues of digital archiving?	This question seeks information about the repository community's access to and sharing of legal information pertaining to their activities.	Go to Q.8

No.	Section 2 - Repository Information and Agreements	Rationale	Pathway
8	Do you require depositors to sign a deposit agreement before supplying material to your archive or repository?	Depositor agreements vary widely between repositories, and it is not unknown for deposits to be made without any formal written agreement. Samples could/should be obtained from focus group members.	If YES go to Q.9 If NO go to Q.12
9	Do you provide guidance on the legal and ethical conditions your deposit agreement contains?	Deposit agreements, the implications of which are insufficiently explained to depositors, are inevitably going to be less effective at helping repositories avoid legal difficulties. However the extent of the guidance perceived as necessary is likely to vary.	Go to Q.10
10	Do you believe that the average depositor understands the legal/ethical implications of conditions contained in such deposit agreements?	Evidence of depositor comprehension here would be helpful	Go to Q.11
11	Can depositors easily negotiate the conditions under which you accept digital materials?	This question seeks to elicit how flexible repositories are in their deposit processes. The more flexible a repository is the more material it can potentially accept, but the process of administrating the repository will become more complex. The perceived trade-off may be interesting.	Go to Q.12
12	Do you accept electronic deposit of digital materials?	Electronic deposit can cause problems , particularly in ensuring that depositors have read and understood deposit agreements.	Go to Q.13

No.	Section 3 - Use and Re-use of Archive Material	Rationale	Pathway
13	Do you require users to sign a user agreement before accessing material in your archive or repository?	Most repositories appear to have some form of user agreement that it is required to sign up to before accessing materials. There may, however, be differences between the conditions for access to digital/non-digital materials.	Go to Q.14
14	Do you provide users with explicit guidance on appropriate use and re-use of archive material?	User agreements, the implications of which are insufficiently explained to users, are inevitably going to be less effective at helping repositories avoid legal difficulties. However the extent of the guidance perceived as necessary is likely to vary.	Go to Q.15
15	Do you believe that the average depositor understands the legal/ethical implications of conditions contained in such deposit agreements?	There are two key issues here: whether users fully understand the legal and ethical implications of conditions in user agreements they sign up to; and whether they care.	Go to Q.16
16	Have you refused access to a personal digital archive in your collection on the ground that the proposed use/re-use would raise legal/ethical issues not envisaged by the depositor?	This is seeking non-standard case scenarios for access refusal on legal/ethical grounds.	Go to Q.17
17	In your experience, when using digital material received by your archive/repository from private individuals, do users follow the relevant conditions for its use strictly?	In essence, this is asking whether repositories believe that their user agreements are observed in practice - there may be some scope for examining scenarios where use conditions are ignored, and effectiveness o f sanctions that are available to a repository.	Go to Q.18
18	Are you aware of the use of any digital material, received by your archive/repository from private individuals, which has resulted in complaints either by the depositor or by third parties?	There is a lot of concern expressed about the legal/ethical issues around digital material provided by private individuals. What there appears to be relatively little of is evidence that there is a significant problem. This should tie in with questions in the archiver-depositor and user interview schedules.	Go to Q.19

No.	Section 4 - Adding Value to Archive Material	Follow-ups	Pathway
19	Does your archive/repository support legal metadata for issues such as copyright ownership and licensing information, or data protection status?	Use of metadata varies across archives and repositories. Personal digital archives are likely to provide particularly complex issues due to the varied nature of material deposited. Information about use of legal metadata seems relatively thin.	If YES go to Q.20 If NO go to Q.22
20	Do you find that digital material received by your archive/repository from private individuals currently comes with adequate metadata to enable effective and efficient use of the material?	As per Q.19	Go to Q.21
21	Do you provide guidance to would-be depositors on how to add metadata to their digital archives?	Some repositories in other areas of activity do provide specific guidance about use of metadata, and some may refuse to accept materials that are not at least tagged with key metadata elements.	Go to Q.22
22	Do you think that the publicity surrounding data protection and copyright issues on the internet has had an influence on the way in which the use and reuse of digital material in repositories is treated?	Essentially is the rise in public perception about intellectual property rights and privacy rights having a noticeable knock-on effect in terms of the conditions placed on the use and re-use of digital materials in repositories?	Go to Q.23

No.	Section 5 - Adding Value to Archive Material	Follow-ups	Pathway
23	How do you think that repositories could most effectively improve the usefulness of digital material provided by private individuals?	This aims to get interviewees/focus group members to assess how they think current repository practices could be improved, in terms of communication about legal/ethical issues with users and depositors, with the aim of improving the quality of material (and metadata) provided for inclusion in repositories, and ensuring that legal/ethical requirements for use are met.	Go to Q.24
24	Would some form of symbolic representation indicating appropriate use of digital material be helpful?	The aim here is to assess whether repositories consider that such mechanisms are useful in simplifying the use/reuse of digital material.	Go to Q.25
25	If you could change one thing about the law relating to your work in archives/repositories, what would it be?		END

PDArcs - Depositors/Self-archivists - Interview Schedule

No.	Section 1 - Creating your archive	Follow-ups	Pathway
1	Did you set out to create a personal archive, or was archiving a later decision?	What, or who, triggered the decision to archive?	Go to Q.2
2	How important have legal issues been in the construction of your archive?	Who was the archive intended for?	Go to Q.3
3	When you began archiving material, did you consider the legal or ethical issues that might arise from your archiving?	What issues did you consider? Did you seek advice on those issues? From which sources? Did you obtain useful/accurate answers to your questions? Have you excluded material from your archive because of uncertainty about legal issues?	Go to Q.4
4	What types of copyright works are contained in your archive?	New solely authored works by you; New jointly authored works by you; Works created by 3rd parties For third party works are they: public domain; no licence; restrictive licence; open licence; unknown rightsholder. Have you ever sought permission to include the © works of others in your personal archive? When? Why?	Go to Q.5
5	Are there privacy, data protection, or confidentiality issues with items in your archive?	Do you think that others might object to the deposit of items in your archive with a publically accessible repository? Why?	Go to Q.6
6	Do you have any other legal/ethical concerns about your archive?		Go to Q.7
7	Have you recorded information about items in your archive, e.g. © clearances, permission to use private material, requests for temporary or permanent confidentiality?	Do you use a formal system for recording this information? If provided with a 'good practice' system would you use it?	Go to Q.8

No.	Section 2 - Depositing your archive	Follow-ups	Pathway
8	When considering deposit of personal archives, were legal/ethical considerations important in your decision to deposit, or influential in your choice of repository?	When did you decide to deposit the archive? Was deposit always the intended aim behind creating the archive?	If YES go to Q.9 If NO go to Q.13
9	Which legal/ethical considerations were relevant to you, e.g. copyright, data protection, confidentiality, other?	Why that/those issue(s) in particular?	Go to Q.10
10	What was your experience of discussing the legal/ethical issues relevant to you with repository institutions? Did repositories appear knowledgeable about the issues you were concerned with?	Was advice given? Was documentation provided? Was that information comprehensible and relevant? What impact did it have on your decision to deposit?	Go to Q.11
11	Did you seek advice on the legal/ethical issues from any other source?	Which sources? Were they helpful? Did you obtain useful/accurate answers to your questions?	Go to Q.12
12	Overall, were you happy with the amount of information available to you regarding your legal considerations?	What would be the most effective source/ mechanism for delivering the information you required?	Go to Q.13
13	Have you excluded materials from your archive during its development or removed them prior to deposit due to legal issues, or other considerations?	What types of material and due to which issues?	Go to Q.14

No.	Section 3 - Deposit Agreements	Follow-ups	Pathway
14	When depositing material were you required to complete a depositor's agreement?		If YES go to Q.15 If NO go to Q.19
15	Did you or an advisor/agent/other person read that agreement in detail?	If not, why not? E.g. too long, too complicated	Go to Q.16
16	Were legal or ethical issues raised in the depositor's agreement?	Which legal or ethical issues?	Go to Q.17
17	Did you understand the implications of those legal issues?	If you did not understand the implications fully, was this a concern?	Go to Q.18
18	Did the depositor's agreement come with explanatory documentation?	Was that information comprehensible? What impact did it have on your decision to deposit? How would you have improved the information provided?	Go to Q.19
19	Were you able to negotiate the conditions under which you deposited material?	Did you negotiate any conditions? Did you seek advice prior to, or during, those negotiations?	Go to Q.20
20	Are there any particular restrictions placed on the use of your deposited archival material?	What are those restrictions? Are they contextual (e.g. material can only be utilised for non-commercial purposes)? Why did you feel them necessary? Were the restrictions available within a depositor's agreement, or were they negotiated separately?	Go to Q.21

No.	Section 4 - Access to, and use of, your archive	Follow-ups	Pathway
21	Is your deposited archival material currently available to the general public, or to specific user groups?	If your deposited archival material is only available to specific users, why is this?	If YES go to Q.22 If NO go to Q.23
22	Has access to your deposited archival material resulted in any complaints from 3rd parties, e.g. on legal grounds?	What type of complaints have arisen? What form did the complaints take? E.g. informal, communication with you, communication with repository, threat of legal action?	Go to Q.23
23	Do you feel that current repository practice in explaining legal issues to depositors is effective, and that current processes for dealing with legal and ethical issues provide sufficient protection to both depositors and 3rd parties?		Go to Q.24
24	Knowing what you know now, what would you do differently as regards the legal implications of your personal archiving and deposit?		END

PDArcs - Depositors/Self-archivists - Interview Schedule background

No.	Section 1 - Creating your archive	Rationale	Pathway
1	Did you set out to create a personal archive, or was archiving a later decision?	How self-archivists come to be self-archivists will affect the timing of consideration of legal issues and may influence the type/timing of repository interactions with depositors.	Go to Q.2
2	How important have legal issues been in the construction of your archive?	This will discuss how the purpose of the archive affects attitudes towards legal issues and additionally provide a snapshot of the scope of legal interventions encountered and the nature of those interventions.	Go to Q.3
3	When you began archiving material, did you consider the legal or ethical issues that might arise from your archiving?	This aims to identify the degree of engagement with legal issues from an early stage. It also seeks to identify where self-archivists turn to for legal/ethical advice, the value of that advice, and its effect on archive content.	Go to Q.4
4	What types of copyright works are contained in your archive?	This aims to gauge the level of © understanding amongst self-archivists, particularly their awareness about their rights and those of third parties, and the implications of © licensing and permissions. Depositors cannot meaningfully complete © statements in deposit agreements if they do not understand the issues involved.	Go to Q.5
5	Are there privacy, data protection, or confidentiality issues with items in your archive?	This aims to gauge the level of privacy understanding amongst self-archivists, particularly their awareness about their rights and those of third parties. IT may be possible to explore whether they consider 3rd party objections to archiving of such data to be 'reasonable'.	Go to Q.6
6	Do you have any other legal/ethical concerns about your archive?	© and privacy are key issues, but it will be important to identify other potential legal/ ethical issues that both self-archivists and repositories may need to consider when planning a new archive or preparing an archive for accession by a repository.	Go to Q.7
7	Have you recorded information about items in your archive, e.g. © clearances, permission to use private material, requests for temporary or permanent confidentiality?	This question is primarily concerned with 'metadata', although the questions will not refer to it as such. The aim is to establish the degree of acceptability/resistance to use of metadata by self-archivists. In other contexts, it is claimed that the use of Web 2.0 technologies such as 'tagging' has increased acceptance of the value of simple metadata systems amongst potential depositors.	Go to Q.8

No.	Section 2 – Depositing your archive	Rationale	Pathway
8	When considering deposit of personal archives, were legal/ethical considerations important in your decision to deposit, or influential in your choice of repository?	This aims to identify the time at which particular legal considerations are considered by would-be depositors (influenced by the archive's original purpose) and also how they influence depositors' decisions about what to deposit and where to deposit it	If YES go to Q.9 If NO go to Q.13
9	Which legal/ethical considerations were relevant to you, e.g. copyright, data protection, confidentiality, other?	This aims to identify the key legal issues important to depositors, which repositories will need to take into account when drafting deposit agreements and guidance. This may differ significantly across a range of self-archivists.	Go to Q.10
10	What was your experience of discussing the legal/ ethical issues relevant to you with repository institutions? Did repositories appear knowledgeable about the issues you were concerned with?	This seeks to identify the current state of play in terms of self-archivist experiences with repositories. Are repositories meeting the needs of self-archivists for clear and effective guidance on legal and ethical issues at the point of deposit? And is current practice encouraging or dissuading self-archivists from depositing all or some of their material.	Go to Q.11
11	Did you seek advice on the legal/ethical issues from any other source?	This aims to identify where self-archivists turn for advice on handling mature archives, particularly at the point of deposit. It would be helpful to discover the extent to which guidance is informal or formal, e.g. books/colleagues/ internet vs. agent/lawyer.	Go to Q.12
12	Overall, were you happy with the amount of information available to you regarding your legal/ ethical considerations?	This seeks to explore self-archivists' expectations about both where they expect 'good practice' leadership to come from (e.g. repositories), and the technical means by which it might be delivered (e.g. online resources, books, training etc.). It may also help to identify (in conjunction with Q.4, Q.5 & Q.11) the extent to which would-be depositors are able to access useful information, and whether misconceptions about the law are hindering the archiving and deposit process.	Go to Q.13
13	Have you excluded materials from your archive during its development or removed them prior to deposit due to legal issues, or other considerations?	It is useful to get some idea of the material that is being lost to repositories because of concerns about legal issues, and to determine whether or not such losses can be reduced, either by means of more effective guidance about the law, or by drawing up/negotiating deposit agreements that are flexible enough to meet a range of depositor requirements.	Go to Q.14

No.	Section 3 - Deposit Agreements	Rationale	Pathway
14	When depositing material were you required to complete a depositor's agreement?	Depositor agreements vary widely between repositories, and it is not unknown for deposits to be made without any formal written agreement.	If YES go to Q.15 If NO go to Q.19
15	Did you or an advisor/agent/other person read that agreement in detail?	Depositor agreements are a major bone of contention within repositories. There are those that see detailed depositor agreements as likely to put off potential depositors, whilst others feel that it is necessary to cover the full range of legal/ethical issues with depositors. Some depositors are also keen on a precise understanding of what they are agreeing to. The aim is to determine the extent to which such agreements are actually properly/effectively utilised. A multi-level approach (e.g. simple agreement + basic explanation/full agreement + comprehensive explanation) might be most effective at encouraging deposit.	Go to Q.16
16	Were legal or ethical issues raised in the depositor's agreement?	It would be surprising if, in a depositor agreement for a repository there were no provisions for IP rights, privacy, and warranties/ indemnities to protect the repository. The aims is to gauge the extent to which such issues are recognised by depositors (esp. responsibilities placed on them by warranties/ indemnities)	Go to Q.17
17	Did you understand the implications of those legal issues?	As per Q.16	Go to Q.18
18	Did the depositor's agreement come with explanatory documentation?	As per Q.15	Go to Q.19
19	Were you able to negotiate the conditions under which you deposited material?	Many repositories in areas such as e-learning tools, academic research etc. tend to have standardised depositor agreements, and are unwilling to diverge from them. In contrast, it appears that repositories accepting personal archives are much more open to the possibility of accepting 'non-standard' terms through a negotiation process. This process would inevitably be impacted by mechanisms such as e-deposit, where depositor/repository relations are at a distance and incorporating negotiation may be more difficult.	Go to Q.20
20	Are there any particular restrictions placed on the use of your deposited archival material?	The aim here is to generate information on the types of restrictions that self-archivers are likely to favour in their dealings with repositories.	Go to Q.21

No.	Section 4 - Access to, and use of, your archive	Follow-ups	Pathway
21	Is your deposited archival material currently available to the general public, or to specific user groups?	This aims to identify depositor issues about dissemination of information contained in their deposit, including why they might seek to restrict access, e.g. are they concerned about breaches of their privacy, or the privacy of others mentioned in their deposited materials; are they protecting their IP rights or those of 3rd parties etc.	If YES go to Q.22 If NO go to Q.23
22	Has access to your deposited archival material resulted in any complaints from 3rd parties, e.g. on legal grounds?	It would be helpful to be able assess the extent to which self-archiving/deposit has led to practical problems with legal or ethical issues, as opposed to merely theoretical ones. Much of the activity of self-archivers and repositories will be undertaken, consciously or unconsciously, on a risk/benefit assessment basis. It would help to understand whether fears about uses of deposited materials have significant ground in reality.	Go to Q.23
23	Do you feel that current repository practice in explaining legal issues to depositors is effective, and that current processes for dealing with legal and ethical issues provide sufficient protection to both depositors and 3rd parties?	This aims to get interviewees/focus group members to assess how they think current repository practices could be improved, in terms of communication about legal/ethical issues with self-archivers and would-be depositors, with the aim of improving the quality of material (and metadata) provided for inclusion in repositories.	Go to Q.24
24	Knowing what you know now, what would you do differently as regards the legal implications of your personal archiving and deposit?	This aims to get interviewees/focus group members to assess their own practices, past and present, with the aim of eliciting community-based best practice information that can be incorporated into future guidance.	END

PDArcs - Repository Users - Interview Schedule

No.	Section 1 - Accessing Archive Material	Follow-ups	Pathway
1	What are the key legal/ethical issues that affect your use of digital material accessioned by repositories from private individuals?	What types of material do you most commonly seek to access?	Go to Q.2
2	In your field of interest, is digital material accessioned by repositories from private individuals generally made available to the public, usually only made available to particular groups of user (e.g. academics), or otherwise subject to conditions of use/access?	If digital material in your field of interest is often subject to conditions of use, what are those conditions? Do you think they are necessary/reasonable?	Go to Q.3
3	Do legal/ethical issues impact upon knowledge about / discovery of digital material accessioned by repositories from private individuals?	Do legal/ethical-based constraints reduce the knowledge about what material has been archived/will be available in the future? Could this be avoided?	Go to Q.4
4	Have you been prevented from accessing digital material accessioned by repositories from private individuals due to legal/ethical-based constraints?	What are the primary legal/ethical-based reasons for denying access to archival material? Are these reasonable?	Go to Q.5
5	Have you ever sought advice on the legal/ethical issues pertaining to use of digital material accessioned by repositories from private individuals from any other source?	Which sources? Were they helpful? Did you obtain useful/accurate answers to your questions?	Go to Q.6
6	Overall, were you happy with the amount of information available to you regarding your legal considerations?	What would be the most effective source/ mechanism for delivering the information you required?	Go to Q.7
7	Have you ever sought to overturn a decision of a repository to deny access to digital material accessioned from private individuals?	Was this an 'internal appeal ' within the repository, a request to the original donor, a request to a third party with interests in the archived material, or a legal appeal?	Go to Q.8
8	Have you ever sought digital material accessioned by repositories from private individuals via Freedom of Information legislation, or via other legal routes?		Go to Q.9

No.	Section 2 - Repository Agreements	Follow-ups	Pathway
9	Do all of the repositories you use require you to sign a user agreement before accessing material?	Does that user agreement impose different terms for digital/non-digital materials?	If YES go to Q.10 If NO go to Q.13
10	Are you happy that you understand the legal and ethical implications of conditions contained in such user agreements?	If you have not fully understood the implications of some legal/ethical conditions, has this been a concern?	Go to Q.11
11	Have you ever decided not to use digital materials because of the terms and conditions of a repository user agreement?	What types of user agreement term might dissuade you from using digital materials?	Go to Q.12
12	Do you find that user agreements provide clear and effective guidance on the legal and ethical conditions they contain?	Are repositories generally knowledgeable about/able to discuss legal/ethical conditions in the user agreements you are concerned about? Are there particular examples of good practice you would recommend?	Go to Q.13

No.	Section 3 - Use and Re-use of Archive Material	Follow-ups	Pathway
13	Do any of the repositories you use provide guidance on appropriate use and re-use of archive material?	Are there particular examples of good practice you would recommend? Are there any other sources (e.g. professional bodies, funding bodies) that provide useful information?	Go to Q.14
14	In your experience, when using digital material accessioned by repositories from private individuals do users follow the relevant conditions for its use strictly?	If you think users don't always follow the conditions for its use strictly, in what circumstances would you consider them to be most likely to not follow them?	Go to Q.15
15	Are you aware of the use of any digital material accessioned by repositories from private individuals resulting in complaints either by the depositor or by third parties?	Did the conditions for the digital material's use clearly cover the circumstances about which the complaints were made? Were the complaints upheld? If so, what were the consequences? If not, why not?	Go to Q.16
16	Can you provide examples of 'public interest' research that have been hindered or prevented due to legal/ ethical difficulties with using digital materials provided by private individuals?	Are there particular types of digital material that are likely to raise these issues? If so, why?	Go to Q.17
17	Do you find that digital material accessioned by repositories from private individuals currently comes with sufficient metadata to enable effective and efficient use of the material?	Is digital material more or less likely to have useful metadata than non-digital material?	Go to Q.18
18	When accessing digital material accessioned by repositories from private individuals which contains metadata, is that metadata likely to cover legal issues such as copyright ownership and licensing information, or data protection status?	How commonplace is legally-oriented metadata in digital repositories?	Go to Q.19
19	Do you think that the publicity surrounding data protection and copyright issues on the internet has had an influence on the way in which the use and reuse of digital material in repositories is treated?	Do you think that depositors of material in digital repositories are more or less likely to assert intellectual property rights (e.g. copyright) in their deposited materials, than depositors of non-digital materials?	Go to Q.20

No.	Section 4 - Adding Value to Archive Material	Follow-ups	Pathway
20	How do you think that repositories could most effectively improve the usefulness of digital material provided by private individuals?	Is more metadata a solution? Who should provide the metadata, the depositor or the repository? Is there an appropriate standard for metadata for material of this type?	Go to Q.21
21	Would some form of symbolic representation indicating appropriate use of digital material be helpful?	Would a model like that of the Creative Commons symbols be helpful in speeding up decisions about the use of digital material provided by private individuals?	Go to Q.22
22	If you were running a repository, and you wanted to provide the most effective and efficient service to end-users, how would you structure your service?		END

PDArcs – Repository Users – Interview Schedule background

No.	Section 1 – Accessing Archive Material	Rationale	Pathway
1	What are the key legal/ethical issues that affect your use of digital material accessioned by repositories from private individuals?	This aims to identify those legal/ethical issues most important to end users. This may vary depending on the type of digital material to be used, but there are likely to be common themes to explore.	Go to Q.2
2	In your field of interest, is digital material accessioned by repositories from private individuals generally made available to the public, usually only made available to particular groups of user (e.g. academics), or otherwise subject to conditions of use/access?	The degree of control exercised over access to digital materials will influence the degree of control of use and reuse that is then exercised by finer legal tools, such as © and privacy laws. This aims to assess the extent to which 'gross access control' is preferred to 'fine use control'.	Go to Q.3
3	Do legal/ethical issues impact upon knowledge about /discovery of digital material accessioned by repositories from private individuals?	This aims to assess the impact that legal/ethical based controls have on knowledge about deposited material, i.e. the extent to which legal controls prevent users from knowing what will be available at some point in the future – a problem with 'dark' archives.	Go to Q.4
4	Have you been prevented from accessing digital material accessioned by repositories from private individuals due to legal/ethical-based constraints?	This is essentially seeking anecdotal evidence of negative impacts upon research caused by legal constraints. These can then be followed up (probably in Digital Lives II) to assess whether the scale of negative impact justifies action at some level to ameliorate it.	Go to Q.5
5	Have you ever sought advice on the legal/ethical issues pertaining to use of digital material accessioned by repositories from private individuals from any other source?	This aims to identify which sources users go to, to obtain information about legal/ethical issues. It would be helpful to discover the extent to which guidance is informal or formal, as well ascertaining the level of confidence that users place in it.	Go to Q.6
6	Overall, were you happy with the amount of information available to you regarding your legal considerations?	This seeks to explore users' expectations about both where they expect 'good practice' leadership to come from (e.g. repositories, user groups etc.), and the technical means by which it might be delivered (e.g. online resources, books, training etc.). It may also help to identify the extent to which users are able to access appropriate information, and whether misconceptions about the law are deterring users from making effective use of digital materials.	Go to Q.7
7	Have you ever sought to overturn a decision of a repository to deny access to digital material accessioned from private individuals?	Oversight of decisions about access to digital materials will be key to ensuring consistency in repository/user community practice.	Go to Q.8
8	Have you ever sought digital material accessioned by repositories from private individuals via Freedom of Information legislation, or via other legal routes?	Some repositories (part of or attached to 'public authorities', as defined by FOIA) may have a legal obligation to disclose information provided by private individuals. It is unclear how common this practice currently is, or the impact on repository practices.	Go to Q.9

No.	Section 2 – Repository Information and Agreements	Rationale	Pathway
9	Do all of the repositories you use require you to sign a user agreement before accessing material?	Most repositories appear to have some form of user agreement that it is required to sign up to before accessing materials. There may, however, be differences between the conditions for access to digital/non-digital materials.	If YES go to Q.10 If NO go to Q.13
10	Are you happy that you understand the legal and ethical implications of conditions contained in such user agreements?	There are two key issues here: whether users fully understand the legal and ethical implications of conditions in user agreements they sign up to; and whether they care.	Go to Q.11
11	Have you ever decided not to use digital materials because of the terms and conditions of a repository user agreement?	This should also pick up on circumstances where use of digital materials was less effective. The aim is to see what types of T&Cs dissuade potential users, this will permit a cost/benefit assessment of such T&Cs	Go to Q.12
12	Do you find that user agreements provide clear and effective guidance on the legal and ethical conditions they contain?	This aims to ascertain whether repositories are doing an effective job of providing information about legal/ethical conditions to their users. It will feed into assessment as to whether, and how, such information provision can be improved.	Go to Q.13

No.	Section 3 - Use and Re-use of Archive Material	Rationale	Pathway
13	Do any of the repositories you use provide guidance on appropriate use and re-use of archive material?	As per Q.12	Go to Q.14
14	In your experience, when using digital material accessioned by repositories from private individuals do users follow the relevant conditions for its use strictly?	Practice evaluation is an important component of any assessment of the effectiveness of T&Cs. If users do not follow the T&Cs, it's important to know why they don't before one can effectively intervene in and change existing practices, or alternatively alter the T&Cs.	Go to Q.15
15	Are you aware of the use of any digital material accessioned by repositories from private individuals resulting in complaints either by the depositor or by third parties?	There is a lot of concern expressed about the legal/ethical issues around digital material provided by private individuals. What there appears to be relatively little of is evidence that there is a significant problem. This should tie in with questions in the archiver-depositor and archive interview schedules.	Go to Q.16
16	Can you provide examples of 'public interest' research that have been hindered or prevented due to legal/ethical difficulties with using digital materials provided by private individuals?	As per Q.15	Go to Q.17
17	Do you find that digital material accessioned by repositories from private individuals currently comes with sufficient metadata to enable effective and efficient use of the material?	Metadata is another area of considerable debate surrounding digital archives/repositories. Metadata is time-consuming to create, and it has been suggested that requiring it for deposited material may deter would-be depositors. Defending the requirement of metadata really requires a clear demand that it be supplied, and also some idea of the form that it should most usefully take. Metadata standards are a particularly thorny area of debate – determining the level of simplicity that meets user demand avoids specifying unduly complex systems.	Go to Q.18
18	When accessing digital material accessioned by repositories from private individuals which contains metadata, is that metadata likely to cover legal issues such as copyright ownership and licensing information, or data protection status?	As per Q.17	Go to Q.19
19	Do you think that the publicity surrounding data protection and copyright issues on the internet has had an influence on the way in which the use and reuse of digital material in repositories is treated?	Essentially is the rise in public perception about intellectual property rights and privacy rights having a noticeable knock-on effect in terms of the conditions placed on the use and re-use of digital materials in repositories?	Go to Q.20

No.	Section 4 - Adding Value to Archive Material	Follow-ups	Pathway
20	How do you think that repositories could most effectively improve the usefulness of digital material provided by private individuals?	This aims to get interviewees/focus group members to assess how they think current repository practices could be improved, in terms of communication about legal/ ethical issues with users, with the aim of improving the quality of material (and metadata) provided for inclusion in repositories.	Go to Q.21
21	Would some form of symbolic representation or multi-level use metadata indicating appropriate use of digital material be helpful?	The aim here is to assess how much use/ reuse information users require in order to feel comfortable in using/reusing digital material.	Go to Q.22
22	If you were running a repository, and you wanted to provide the most effective and efficient service to end-users, how would you structure your service?	The aim here is to generate information on the types of provisions that users are likely to favour in their dealings with repositories.	END

Arts & Humanities Research Council

Grant Number BLRC 8669