InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems

Policy Cross-domain

Information Policy: Privacy Report

Malcolm Todd
National Archives of the United Kingdom

October 2005
(final revisions July 2008)

Table of Contents

1. Introduction

This summary report encapsulates the principal findings emerging from a number of discrete studies conducted within the Policy Cross-domain of the InterPARES 2 Project and goes on to attempt to match that juridical and strategic level research with the case study data also emerging from the Project, mostly from Focus 3 (e-government activities). (Apart from the last, it is **not** the primary research product).

Citations: [1] InterPARES 2 Project papers published in peer reviewed journals:

- Livia Iacovino and Malcolm Todd (2007), "The long-term preservation of identifiable personal data: a comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada and the United States," *Archival Science* 7(1): 107-127.

- Malcolm Todd (2006), "Power, Identity, Integrity, Authenticity, and the Archives: A Comparative Study of the Application of Archival Methodologies to Contemporary Privacy," *Archivaria* 61 (Spring): 181-214.

Citations: [2] Other InterPARES2 Project papers:

- Luciana Duranti (2005), "InterPARES 2 Project - Policy Cross-domain: Authenticity and Authentication in the Law." http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_law.pdf

- Fiorella Foscarini (compiler) (2005), "InterPARES 2 Project - Policy Cross-domain: Authenticity and Authentication Issues in the Italian and European Union Legislation." http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_it-eu.pdf

- Maria Guercio (2004), "InterPARES 2 Project - Case Study 25 Final Report: Legacoop of Bologna Web Site." http://www.interpares.org/display_file.cfm?doc=ip2_cs25_final_report.pdf

- Livia Iacovino and Malcolm Todd, "Ethical Principles, Accountability and the Long-term Preservation of Identifiable Personal Data: A Comparative Analysis of Privacy Legislation in Australia, Canada, the European Union and the United States," paper presented at the *Association of Canadian Archivists, Ethics and Accountability in the Archival Sphere, 29th Annual Conference, May 26–29, 2004, Montréal, Québec, Canada*. http://www.interpares.org/display_file.cfm?doc=ip2(policy)Iacovino_Todd_Abstract(200406).pdf

- Brent Lee (2005), "InterPARES 2 Project - Domain 2 Task Force: Authenticity, Accuracy and Reliability of Arts-related and Archival Literature," draft discussion paper. http://www.interpares.org/display_file.cfm?doc=ip2_aar_arts_lee.pdf

- John McDonough, Ken Hannigan and Tom Quinlan (2005), "InterPARES 2 Project - Case Study 20 Final Report: Revenue On-Line Service (ROS)." http://www.interpares.org/display_file.cfm?doc=ip2_cs20_final_report.pdf

- John Roeder (2004), "InterPARES 2 Project - Domain 2 Task Force: Authenticity, Accuracy and Reliability of Artworks: A Review of the Literature, with Some Notes about the Challenges Presented by Digital Media," draft version 2. http://www.interpares.org/display_file.cfm?doc=ip2_aar_arts_roeder_v2.pdf

- John Roeder, Philip Eppard, William Underwood and Tracey L. Lauriault, "Part Three - Authenticity, Reliability and Accuracy of Digital Records in the Arts, Science and Government: Domain 2 Task Force Report," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Rome, Italy: Associazione Nazionale Archivistica Italiana, 2008). http://www.interpares.org/display_file.cfm?doc=ip2_book_part_3_domain2.pdf

- Jim Suderman, Fiorella Foscarini and Erin Coulter (2005), "InterPARES 2 Project – Policy Cross-domain: Archives Legislation Study Report." http://www.interpares.org/display_file.cfm?doc=ip2(policy)archives_legislation_study_report.pdf

- Sherry Xie (translator and compiler) (2005), "Policy Cross-Domain: Legislation Study - People's Republic of China (Report III): Access to Information in Chinese Legislation." http://www.interpares.org/display_file.cfm?doc=ip2(policy)archival_legislation_CHINA_ACCESS_TO_INFORMATION.pdf

Citations: [3] Conference and other papers/publications:

- Terry Maxwell, "International Archival E-Policy, Management and Technology," in R. H. Sprague (ed.), *Proceedings of the 39th Hawaii International Conference on System Sciences, 4-6 January 2006, Big Island, Hawaii* (Los Alamitos, CA: IEEE Computer Society, 2006).

Acknowledgements

This report has been compiled by the present author, but the underlying research has been a team effort drawing on a number of resources: Within an international project such as InterPARES, foremost has been the international knowledge of the following archival experts within the Project:

- Maria Guercio, University of Urbino (Italy)
- Isabelle de Lamberterie, Centre Nationale de la recherche scientifique (France)
- Hannelore Dekeyser, Leuven University (Belgium, EU)
- Terry Maxwell, University of Albany, NY (USA, more generally)

The second category is research conducted specifically as component parts of this study or in related papers contemporaneous with the Project (not necessarily within it):

- Livia Iacovino, Monash University
- Terry Maxwell, University of Albany
- Sharon Farb, University of California, Los Angeles
- Jane Morrison, The University of British Columbia
- Sherry Xie, The University of British Columbia

2. Background

The research occurs at a time of dramatic world events causing fundamental change to privacy policies of national, sub-national and supra-national governments. It also coincides—not by any accident—with the type of technological change affecting records creation that is the specific mission of InterPARES 2 to study and to work out the strategies, policies and procedures for ensuring the preservation of authentic digital records from the activities in question.

Matching the two and making sense of the result is difficult and must remain slightly tentative, even at the closing stages of the research. Making recommendations to benefit purely archival ends is also faced with the challenge of far more immediate threat to life and safety. These concerns will inevitably rate higher in the legislative priorities of governments. The highest-level recommendation of this report is therefore one of seeking renewed strategic alliances with other parties and policy agendas. Principal amongst these must be the professionals who also have an interest in the preservation of authentic archival records, whether directly represented in InterPARES or not: scientists (including the social sciences), public servants, and artists. In addition, the need for a restatement of the contribution of archives to the polity as well as the heritage of a modern, pluralist society is a view this report shares with the contemporary work of some others in this area, including political scientists, technologists and other archivists. Beyond that, the implications of this report are of pertinence to the ordinary citizen and raising the awareness of this group to these issues is also important.

We were at a time of legislative innovation in this area before the security situation changed in the second year of the present century and this can be associated as clearly with e-commerce and globalisation as a previous wave could with the emergence of direct marketing and mass commercial data processing in the 1960s and 1970s. eGovernment initiatives are also very much associated with public freedom of information policies. Speaking very broadly, it makes some sense to associate these drivers with our experiential, dynamic and interactive record creation environments. Making a case for Archival purposes in this environment and faced with these fundamental issues is thus a challenging task, as is borne out by the analysis of the records creation environment observed in the case studies.

3. Research Questions

The scope of the study: primary research question

This study was mandated in September 2004 with reporting on "What are the barriers to the preservation of authentic digital records emanating from privacy protection." This report and the other InterPARES research papers it draws upon have been brought together to fulfil this mandate.

InterPARES original research questions [Policy Cross-domain]

The Policy Cross-domain is responsible for the formulation of policies, strategies and procedures for the creation, maintenance, appraisal and preservation of the records generated in the

technological environments and economic sectors studied by this Project.[1] The research questions assigned to the Policy Cross-domain in the original research proposal of this second phase of the InterPARES Project are [*present author's emphasis*]:

- To what extent do policies, procedures, and standards currently control records creation, maintenance, preservation and use in each focus area? Do these policies, procedures, and standards need to be modified or augmented?
- Can an intellectual framework or frameworks be developed to facilitate the translation of policies, procedures, and standards into different national environments, sectors, and domains?
- How can enhanced control over and standardization of records creation, maintenance, preservation, access and use be balanced against cultural and juridical differences and perspectives on issues such as freedom of expression, moral rights, privacy, and national security?
- What legal or moral obligations exist regarding the creation, maintenance, preservation, and use of the records of artistic and scientific activities?
- What principles should guide the formulation of policies, strategies and standards related to the creation of reliable, accurate and authentic records in the digital environments under investigation?
- What principles should guide the formulation of policies, strategies and standards related to the appraisal of those records?
- What principles should guide the formulation of policies, strategies and standards related to the long-term preservation of those records?
- What should be the criteria for developing national policies, strategies and standards?
- What should be the criteria for developing organizational policies, strategies and standards?

Potentially, privacy regulation bears on all of these research questions in some way. The emboldened text contained in the third and fourth, though, is centrally concerned with these questions. In addition, privacy requires to be seen in the context of other information policy agendas (such as Freedom of Information) and this is the approach taken in the studies. Examining privacy enactments without also considering other requirements to make the content and / or the description of records publicly available would be a futile exercise. There are also important links to access provisions in archival legislation—an obvious but not the only area of overlap with the contemporaneous Archival Legislation study.[2]

[1] For examination of the case study data gathered in response to relevant related research questions in the case studies, refer to section 8, below.

[2] See Suderman, Foscarini and Coulter (2005). Unlike Archival Legislation, no freestanding studies of either FOIA or security have been conducted, but the constituent parts of this study have attempted to draw the boundaries between these areas of information policy.

4. Methodology

Interdisciplinarity and application of the InterPARES 2 intellectual framework

This report is primarily the result of public policy level study of regulatory models and an examination of archival methodology and concepts. The research data arising from the InterPARES 2 case studies has been brought in at a relatively late stage, for reasons of sequencing and the case study coverage (see discussion of this below). Case studies form the most significant area of enquiry and research data of the Project. Accordingly, it was not possible to await the outcome of case studies before beginning research.

An interdisciplinary and comparative methodological approach has been taken to this subject. 'Interdisciplinary' in the sense that the methodologies used have been from both archival and other related professional disciplines; 'comparative' similarly and in that within and without the archival and archival / diplomatic concepts dominant in the intellectual framework of InterPARES 2, the research has always concentrated on possible interface and synergy between different approaches. It has been constructive and fascinating to observe the interplay between different archival traditions and approaches to this subject: the continuum viewpoint has been particularly useful in this respect.

The non-archival disciplines have not in the main been the additional sectors of the economy taken within the ambit of the second phase of InterPARES to supplement more traditional archival environments of the first phase: namely the arts and the sciences. Rather these approaches are best characterised as: juridical, regulatory / bureaucratic, political and social scientific, empirical and postmodern[3] (philosophical).

It will be observed that some of the latter are both archival and extra-archival approaches as they have been used in this research. This is in the nature of the subject matter. Much of the archival professional literature on privacy is by its very nature also of a social and political scientific nature: stressing the professional methodologies of appraisal and access management (the latter often shading into professional ethical and philosophical concerns) and with an inevitable overlap with the effects of the archives on society and their role within it. This approach has been dominant within only one of the studies forming the basis for this report.[4] Instead, an attempt has been made to centre the research on areas more directly affecting the *preservation* of *authentic* digital records and the intellectual framework of the Project.[5] Whilst this has led to some of the privacy research to be conducted from unusual angles, it is hoped that this will be of interest and value to the study of privacy by others.

[3] Individual comments emanating from scientific and artistic concerns are mentioned above in the context of strategic alliances and are contained below.
[4] Maxwell (2006).
[5] That said, beyond identifying challenges to archival appraisal raised by this subject, the main responsibility of Domain 3 of the Project to tackle this area has been respected.

Phases of research

Comparative study across jurisdictions has been a complex undertaking. A broad but by no means comprehensive study has been the first focus of the study of privacy.[6] This concentrated on the EU, USA, Canada and Australia. Even for an international project such as InterPARES this was a major undertaking. Many technical and conceptual archival issues were thrown up within this study that had to be put to one side pro tem to permit the completion of the regulatory comparison work.

The second study expanded the remit of the research from mapping the juridical and empirical archival issues into areas of philosophy and archival theory. Whilst all of these have political dimensions, the final destination is, arguably, precisely where the argument belongs and where the policy recommendations will ultimately germinate. The intellectual framework of the research, though, remained that of archival science.

Finally, in this report, the case study data has been integrated into this higher-level study. There has not been enough case study data and it has not arisen in any quantity early enough in the Project to bear any great weight in its own right, but insofar as it exists it appears to validate other findings. In addition, further areas of suggested research are proposed.

5. Research Findings

The joint consequences of technological advance and privacy protection unqualified by these considerations of archival policy would be to reduce the preservation of authentic digital records to a 'primitive' state.[7] It is possible that the present security agendas of governments might afford some relief to these tendencies, but this must be in some doubt.[8] InterPARES 1 established that digital records are unlikely to survive serendipitously and there is no guarantee that archival and security agendas can be aligned as easily as in the past, where generous closure periods and less regulated retention were the norm.

Policy recommendations

The following series of significant policy recommendations has emerged from the studies:

1. **No single definition of privacy; need to monitor both statute and case law.**

   Despite the tendency towards globalisation of jurisprudence and policy in this area, in the course of the study, it was observed that there was no single definition of privacy[9] (there is

[6] Iacovino and Todd (2007).
[7] This adjective has been employed deliberately to suggest a correlation between the characterisation in Todd (2006) of a 'pre-modern' archival system without requiring the present reader to accept the discussion of the power relationships and postmodern discussions employed in that paper.
[8] The continuance of this approach might continue to be feasible in the United States, for example and may be for the time being in China whereas it is not in the European Union. The caveat needs to be entered, though, that the picture is increasingly a global one. See p. 12.
[9] The most extreme example being the Chinese where openness legislation requires exceptions for personal information without defining what this means. See: Xie (2005).

not even uniformity on whether privacy protection can apply to the dead or entities other than natural persons or 'organic' groups likely to be recognised juridically, such as the family[10]). Whilst it is hardly appropriate for this report to recommend that there should be any such thing, this is an area for archivists to observe developments in case law carefully. Given the fundamental nature of the threat to the archival mission, there may be a role for an international archival body such as the International Council on Archives to create a privacy watchdog. National case law is likely to be of significance in other jurisdictions and this may apply not just in multi-jurisdictional contexts, but also where increasingly global commercial activity is subject to privacy regulation.

In the increasingly distributed environments studied in InterPARES 2, extensions to the definition of privacy beyond the individual or the organic unit such as the family may prove of significance in the survival of, *inter alia*, complex distributed collaborative artwork and a factor in determining whether an individual's mere participation in such an event can constitute them putting it into the public domain and hence their consent for it to be preserved (by reconstruction).[11]

2. Legislative frameworks need *explicitly* to make adequate provision for archival activities.

2a. At the time of writing, many legislative frameworks require revision and greater integration of issues of privacy, Freedom of Information, archival access. This may be done through the articulation of a clear archival exemption that recognises clearly the need to respect the integrity, identity and authenticity of digital records. For example, if there are general duties to update "data," it must be clear beyond doubt that these do not apply to the archives. Such an exemption may be tied to purposes or institutions but the implications of this must be thought through in terms of the jurisdiction's archives model.

Many jurisdictions that have been active on the previous points have only done so insofar as they relates to public records or public archival institutional custody. Although the studies have been primarily about public archives, there is significant worry about the position of private archives in this emerging world.[12] Where public policy permits, this requires attention. Demonstration of compatible purposes is required (see above) unless there is a clear archival override to the duty to dispose/anonymise makes enhanced consent procedures for private archival deposit imperative. This is not a simple matter.

[10] The main vehicle for privacy protection in many jurisdictions is legislation on the protection of personal data and it is often the precise detail of this that most immediately concerns the archivist. Some "Privacy Acts" do little more than this. Iacovino and Todd (2007) found that the relationship between privacy and data protection in the European Union was by no means straightforward with *de jure* privacy protection appearing to go far beyond data protection and—more strangely—EU institutions with data protection remit having a *de facto* effect on privacy protection. For more on the living / dead issue, refer also to the ethical issues recommendation below (see policy recommendation 3 in section 5).

[11] Private e-mail exchange with Andrew Rodger of Library and Archives Canada and InterPARES Artistic Focus, June 2004. In general, the revelation of self inherent in many art forms—including digital ones—would be covered by the normal exception to privacy protection where the individuals have themselves put the information into the public domain. The disclosure of information about others has always been in the background of this, but virtual communities may produce privacy case law of this new kind in the future (see final section of this report).

[12] The Canadian Federal "Total archives" approach is a preferred approach. Privacy laws such as the *Irish Data Protection Act* give no certain valuable processing privileges only to National Archives to process personal information.

Integration of the archives in information policy (access) regimes is required in such a way as to respect the integrity (identity, authenticity) of the Archives, especially problematic with Freedom of Information regimes normally applying to public sector information. This is particularly important if decontextualised, incomplete archives are being made available in any quantity online, especially over the internet as it serves to make authentic preservation irrelevant in the eyes of many. This may mean archives accepting being principal agents of FOI, if public policy allows.

With further regard to the private sector: a number of the studies showed an immaturity in the privacy regulation of the private sector, most notably the United States of America. It is likely that this will be addressed in policy in the future: vigilance will be required on the part of the archival profession on how this will affect archival purposes.

2b. If the archival exemption is articulated in terms of purposes compatible with the original purpose of the data being collected and used, a wide rather than narrow definition of 'compatible [archival] purposes' is preferable. Similarly recognition is required that some archival 'processing' of personal information (e.g., preservation activities such as retention and migration) is of a lesser order of processing than taking business decisions affecting the individual to whom the information relates. It may be preferable to define these as concepts in the law distinct from 'processing' to facilitate this.

This is essential for the survival and flourishing of the archival mission in the present environment and may be required even where there are specific archival exemptions to data protection legislation in place. Where there is a need for both, care must be taken not to make the primacy of the provisions ambiguous.[13]

2c. Many archival laws and regulations have lagged behind innovation in the privacy area and there is ambiguity about primacy of provisions.

For example, in the EU jurisdiction the right to privacy may be wider than the right to data protection and there may be overriding juridical presumptions about proportionality of processing yet to be clarified by case law. These issues need to be resolved as far as possible to the benefit of archival preservation (this is a direct linkage to the Archival legislation study of the Policy Cross-domain). Archivists must be aware that an archival exemption, even where such a thing exists, is unlikely to operate as a blanket provision (see above).

3. Integration of ethical issues in archival access is required, especially by the use of ethical researcher codes. Scope for these has been squeezed and may now have to deal with extremely difficult areas.

These put the onus of research ethics on the researcher by the introduction of undertakings. The Italian deontological code is a model in this respect. This is a particularly difficult area: additional regulation has tended both to reduce the scope and to deepen the complexity of resolving competing ethical concerns. For example, as recommended above, it is desirable

[13] It is incumbent on archival institutions not to abuse such privileges where/if they are granted and this may require a stiffening of professional ethical codes. See below.

for issues of archival access to be properly resolved with the freedom of information and privacy enactments (an issue partly for the archival legislation study). Multiple enactments in many jurisdictions have tended to reduce the scope for ethical decision making to a core of very difficult issues (an ethical decision is by strict definition *not* a legal imperative). Implementation of Freedom of Information policies usually requires a balancing tightening of privacy protection:[14] this can remove some accustomed discretion in ethical access arbitration by the archives and it may not be possible to deem researcher access to be outside aspects of the statutory access regime.

Privacy in many jurisdictions used only to relate to the living individual; this is not necessarily still the case. For example, in the United Kingdom archives legislation used to provide a mechanism for the closure of records whose release would cause "substantial distress," a definition not confined to the data subject alone but potentially to others such as relatives.[15] Data protection cannot extend in the UK beyond the life of the data subject.[16] Access to information contained in the records is in general either covered by the *Data Protection Act 1998*—the personal data—or the *FOIA 2000*—the remainder. Any ethical decision-making in response to an access request is thus shifted onto the less charted territory of human rights law or far tougher tests of actual harm.[17] This is difficult enough where access is requested by a third party, still more yet if requested by a member of the family itself likely to be distressed or harmed by the archives should they comply.[18]

More widely, scientific advance in areas such as genetic profiling and its use by both governments and commercial organisations (e.g., the insurance industry) increases the likelihood of personal information requiring some degree of protection beyond the life of the original data subject as also pertaining to those still living.

4. There is a blurring of the public / private by use of intermediaries / contracting out by governments, with profound and worrying consequences

This is a general issue with a very broad effect of increasing the likelihood of enhanced private sector privacy regulation in the near future at the same time as increasing fears of 'leakage' of personal information from government to commercial organisations.

[14] As observed by Xie (2005), this is seen in somewhat embryonic measures in China designed to comply with World Trade Organisation requirements.

[15] *Public Records Act 1958*, s.3, provided for this to be done over and above the statutory standard closure period by the mechanism of an instrument of the responsible Minister on the recommendation of his Advisory Council on Public Records. Access provisions are now those set by the *FOIA 2000*.

[16] The definition refers to living identifiable individuals.

[17] Article 8 of the European Convention on Human Rights (ECHR) reads: *Everyone has the right to respect for his private and family life, his home and his correspondence…. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the protection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others* (Council of Europe (2003), "Convention for the Protection of Human Rights and Fundamental Freedoms, 213 U.N.T.S. 222, entered into force Sept. 3, 1953, as amended by Protocol No. 11 with Protocol Nos. 1, 4, 6, 7, 12 and 13." http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf).

[18] The type of frankly paternalistic approach possible under the previous regime would be completely at odds with public policy on Freedom of Information, but as the example illustrates this does not exonerate the archivist from an ethical judgement in extreme cases although it does reduce his/her discretion severely. Part of the problem is that the requester's right to Freedom of Information may be at odds with his/her right not to be harmed by that right being recognised. It is complicated further by the difficulty of counselling the requester effectively without first releasing the records.

This is particularly complex and problematic where the means of identification—of citizen in the transaction, then agents in the record creation process—is dependent on a personal identifier that InterPARES 1 established could not be preserved: the third party Public Key Infrastructure digital signature.[19] Similar issues may exist with eGovernment identifiers. These points raise some profound philosophical debates outside the scope of this report, but ones requiring participation from archivists (albeit see the last two recommendations below).

5. Additional urgency is added to that identified in the InterPARES1 Appraisal Task Force reports for the early identification of archives of historical value *and their transfer to archival custody*

Information policy agendas insisting on a clear, compatible justification for the continued processing of personal information, such as privacy, narrow the 'window' for these activities further. If the appraisal decision is not taken before the initial mandate for processing the personal information expires (i.e., whilst the records are still in active use), the legality of its retention may also expire. In addition to this requirement, some regulatory regimes—especially those that link concessions to archival purposes to an institution or even physical custody in particular facilities—seem to require early archival transfer.

6. Archival policies and practices must be sensitive to the difficulties of balancing the ambiguous position of the public archives

The debate about whether it serves the profession to be part of the bureaucracy or semi-detached from it continues:

- Removal from central bureaucracies would undercut many of the juridical devices under which archival processing of personal information is justified. It would also detach the records management and archival agendas whilst InterPARES research recommends specific intervention in the records creation environment to promote preservation.
- There is general mistrust and cynicism about governments' respect for the privacy of citizens at the time of writing. Accordingly, against that is the validity of the 'archives as governance' argument where too close a relationship with power is eschewed in favour of a quasi-independent, 'trusted custodian' status. This might have the potential to increase trust in archival processing of personal information, but would require very substantial legislative change in most jurisdictions.
- *This is arguable both ways: where is the best placement for an individual institution and how does this impact the profession as a whole? For some of us, this maps closely to the theoretical standpoint we adopt as archivists. Much of this argument lies outside the scope of the Report but its relationship with Privacy must be noted as the issue is handed to the Archival Legislation study area.*
- *It should nonetheless be observed that the most important point is that whatever the exact constitution of the archival institution, it must balance that placement with sensitivity to the opposing viewpoint. For example: if it is clearly a part of the*

[19] Two Authenticity studies produced within the Policy Cross-domain tackle the issues where juridical requirements for all official documents to bear digital signatures exist: see Duranti (2005) and Foscarini (2005).

bureaucracy, it must address a governance and accountability agenda (it may be more difficult to do the reverse owing to impaired influence). In any case, its own administration of privacy over its own holdings must be scrupulous (see issues of trust in digital records below).

7. Contribution of the archives to building Digital *Trust*

Archival institutions have a significant role to play and should participate in initiatives to build public trust in archival processing of personal information. In public records regimes these should be integral to eGovernment 'trust charters,' etc. Again, this is two-fold: as strategic players in information management and policy and as processors of personal data ourselves. There should be transparency to the citizen on both these points.

6. Strategies / Ways Forward

Addressing of preceding recommendations

The eleven recommendations in the previous section are highly demanding even as they point the way for the preservation of authentic digital records in contemporary technological environments and public information policy agendas. It is difficult to see how the archival profession can achieve the preceding in isolation. The InterPARES Project has demonstrated the great value of interdisciplinary exchange. The study of this area of information policy in particular shows the benefit—indeed the necessity—of a balancing a plurality of approaches.

Building of strategic interdisciplinary alliances

In addition to the traditional stress on access management and professional ethics, other strategic alliances are now required and a period of vigilance of how these issues play themselves out in public policy over the next few years.

In adopting an interdisciplinary approach to the research, InterPARES 2 has noted the divergence between the archival and diplomatic scientific definitions of authenticity, accuracy and reliability from those in the arts and the sciences.[20] This study validates the utility and indeed the imperative of these interdisciplinary relationships by evolving the same message out of our relationships with the social and political sciences.

These relationships already exist in terms of the usage of archives and the existing archival privacy literature centring itself on this interface. At the theoretical level, though, the relationships have not traditionally been nurtured so assiduously as those with juridical constructs. At this juncture, mutual understanding and pursuit of common interests are essential.

There is a discussion that has begun within the second phase of the InterPARES 2 Project between multidisciplinary views of authenticity, reliability, and accuracy. Archivists must make

[20] See Lee (2005), Roeder (2004) and Roeder et al. (2008). The latter is report of the Domain 2 Task Force, which was concerned with authenticity.

the point that the use of archives for secondary purposes should be informed by the provenance and authenticity of the archives in terms of the primary purpose of the records creator. It is only in understanding this that judgements on the applicability to secondary purposes can be evaluated.

Guarding against a 'pre-modern' archival situation where the archives are not seen as vital to governance, accountability and patrimonial rights owing to the inability to appraise, preserve and otherwise to process archives containing personal data.

The archival profession must also be vigorous in arguing against an imbalanced view of the public and private spheres where the latter is dominant and personal data overprotected. The danger of such an approach is that the public will and public action in respect of private matters becomes opaque and is not subject in the short term to independent audit and eventual, incremental release of archival material as in the past.

7. Analysis of Main Trends

Tendency towards globalisation, but with qualifications

eGovernment implementation and the emergence of global commerce have demanded a regulatory legislative response in most jurisdictions to reassure citizens that their personal information is only to be used for specified purposes. The principles of jurisprudence lying behind this remain as they have been for over a decade and are well analysed in standard texts on the subject such as MacNeil's *Without Consent*.[21] Exactly what form this protection takes varies quite widely.

There have been some remarkable tendencies towards globalisation arising in the main from legislative activity in the European Union, which has become the world's largest trading bloc during InterPARES 2. One important finding to qualify this is the contrast between the generally weak privacy protection in the United States of America compared to elsewhere.[22]

One feature of the legislation is that it is complicated by multijurisdictional instruments. This leads to differences in privacy protection, for example in Australia.[23] In some other jurisdictions, the various levels are a feature of a harmonisation process. The EU Data Protection directive is the clearest and most influential example of this. Even in this case, whilst an EU-wide working party examines privacy protection in extra-European jurisdictions prior to their being approved as places for the processing of personal data about EU citizens, domestic enactments of the Directive vary considerably. Iacovino and Todd found wide variation on how this could affect the archives. In addition, the interplay with the European Convention on Human Rights

[21] Heather MacNeil, *Without Consent: The Ethics of Disclosing Personal Information in Public Archives* (Metuchen, N.J.: Scarecrow Press, 1992).
[22] That is, of the jurisdictions present in the comparative regulatory study; protection in China is clearly weaker still. See Xie (2005).
[23] See Iacovino and Todd (2007), pp. 122-124.

(principally Article 8) as enacted domestically and as appealable to the European Court is complex and clarity may only emerge with more case law.[24]
It remains to be seen whether the horse-trading over national security data (passenger movement records are a particularly immediate example in the post '9/11' world) and the commercial imperative for US companies and subsidiaries to use personal data about EU citizens will lead to any harmonisation of the US jurisdiction or *ad hoc* corporate arrangements[25] by global corporations.

Technical archival issues: personal and record identity

The need to manage the constituent parts of records at the sub-record level—also a feature of many freedom of information regimes—introduces a tension with the integrity, identity of the authentic record as understood by InterPARES research[26] and particularly affecting personal data. This has been the second focus of the research activity on this subject. This is exacerbated technically by the increasing complexity observed in the records creation environments of InterPARES 2. As a result of the challenges posed by these issues, the more traditional areas of archival research on privacy, well known from a substantial literature, have been comparatively neglected.[27]

The paper feeding into this study focussing on the role of personal information within authentic digital archives examines the interplay between content and formal attributes of the records, as well as with the participants in both the business transaction and the record creation process. This is informed by both Diplomatic and Continuum viewpoints and is partly a high-level description issue to be fed to the Description Cross-domain.

Part of the present uncertainty arises from there having developed a somewhat broader definition of what constitutes personal information that may require protection than hitherto. In the European Union jurisdictions the Directive 95/46/EC leaves some uncertainty about what exactly is "personal information." National case law is emerging that suggests that the presence of identifying data in or attached to the record as a result of participation in either the record creation process or the business transaction does not of itself constitute personal data.[28] It remains to be seen whether this will ultimately be the effect of the Directive but this gives a little reassurance that the worst-case scenario that could arise for the archives from this regime of increased privacy protection may be averted. Todd (2006) also argues that the very broadest

[24] Domestic enactment in member states, such as was delayed in the UK until 2000, was mainly to ensure citizens of signatory countries could seek redress through the domestic courts. Ultimately the remaining role of the European Court may be to judge the domestic enactment itself.
[25] Witness the activities of the "Section 29 working party" charged mainly with examining other jurisdiction's protection and making recommendations as to whether it is analogous to that provided in member states but also with examining broader issues than the Directive can arguably bear. See Iacovino and Todd (2007).
[26] See Heather MacNeil, et al., "Part One – Establishing and Maintaining Trust in Electronic Records: Authenticity Task Force Report," in *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Italy: Archilab, 2005), 19–65. Online reprint available at http://www.interpares.org/book/interpares_book_d_part1.pdf. See also Todd (2006).
[27] Albeit not in Terry Maxwell's (2006) pragmatic proposals for achieving some automation of resolving access conflicts in *proposed methodology to automate some of processes to support access decision making in a complex information policy environment*.
[28] Durant vs. Financial Services Authority 2003. See http://www.informationcommissioner.gov.uk for valuable commentary.

definition of personal data would serve to defeat accountability and other aspects of a civilised pluralist democratic society and this is a view shared with recent work by Heather MacNeil.[29]

However, as noted by Luciana Duranti in 1998,[30] the participants in the record creation process are very often the same as either (or both) the data subject and the participants in the activity. The implications of the contextualisation effect of such personal data (as well as other attributes) have also been discussed as a means of carrying forward some of the benchmark requirements of InterPARES1 Authenticity Task Force ('ATF').

Todd (2006, pp. 188-191) suggests that whilst the ATF pronounced that the presence of a higher proportion of the benchmark requirements supported a higher presumption of authenticity, the presence of the attributes of the participants ought to be seen as a *sine qua non* of an authentic record. This presents a professional conundrum: the ATF report rejected a typology of authenticity and preferred a relativist approach but this last point seems to suggest that some attributes are 'more equal than others.' This may require further study.

Technical archival issues: lifecycle

Archives used to be the relatively 'passive' recipients of records whose business purposes declined along a linear route and shaded, eventually, into an historical purpose or purposes. Whilst it has been observed in the studies contributing to this report that juridical enactments tend to replicate the notion of a lifecycle or lifecycles, this requires some consideration.

Archives—particularly in the digital environment—can no longer be seen as merely the recipients of records containing personal data that they can simply retain until "Sunset" clauses have kicked in and the sensitivity / privacy issues of the personal information have ceased, after which they are at liberty to release the entire record with complete impunity. It does not take a doctrinaire interest in records continuum theory to appreciate this point.

This is in part because archives are themselves processors and distributors of personal information that may be reused. This point has received some juridical recognition in the wide definition of "processing" of personal information under the EU directive, a definition with wider international importance as we have seen. Instead, it is more relevant to consider modifying our role to that of a "trusted custodian."[31] Traces of the consequences of such a viewpoint can e found throughout the recommendations of this report.

[29] See Heather MacNeil, "Information Privacy, Liberty, and Democracy," in Menzi L. Behrnd-Klodt and Peter J. Wosh, eds., *Privacy and Confidentiality Perspectives: Archivists and Archival Records* (Chicago: Society of American Archivists, 2005), pp. 67-81.

[30] See Luciana Duranti, *Diplomatics: New Uses for an Old Science* (Lanham, Maryland and London: The Scarecrow Press in association with the Society of American Archivists and the Association of Canadian Archivists, 1998).

[31] Individual enactments vary on the point, even in the multi-jurisdictional framework of the European Union. For example, some states afford particular exemptions to specific types of archival processing, such as giving access to archives users (see discussion of ethical researcher codes in policy recommendation 3 in section 5). The fact remains that Iacovino and Todd (2007) noted the ambiguity over whether historical and research processing and its exceptions trump the data protection processing principles in the EU Directive, and/or in the various enactments of member states, which are differently articulated. This is only likely to be resolved by case law.

On the other hand, both Iacovino and Todd (2006) and Todd (2006) observe that whilst certain aspects of data protection regulation in the European Union might best be understood in terms of all purposes of records being identified *ab initio* and managed as a continuous and simultaneous set of purposes (i.e., tending towards a continuum viewpoint) this is not something that is explicit in the drafting of the laws. Instead, there seems to be a presumption that there does indeed come a time when only purely "historical" or "research" purposes remain, taking us back to the lifecycle model.

One possible resolution of this conceptual issue might be to consider each (re)use or dissemination of personal information as a lifecycle in its own right. This is beyond the scope of this study and insofar as it relates to public archives, is flagged here for the attention of the Archives Legislation study investigators.[32]

Data matching and eGovernment identifiers

More complex computing environments inherent in dynamic, interactive and experiential record making environments are likely to be distributed, the records fragmented and difficult to manage owing to the challenges of definition and description examined elsewhere in InterPARES research. The means of addressing these issues deriving from our own profession but also business process management, data architecture and records management is to link related but otherwise disparate data together. Indeed this may in many environments be the only possible manifestation of a conceptual "record."[33]

The research has also identified broader and more philosophical data matching requirements fundamental to our professional mission: Todd (2006) proposes that our own practices and those of records managers have data matching at their very roots in aggregation principles. It may be different in degree to governments using a single identifier to tag all interactions with one citizen and / or to associate with identity cards or digital signatures but not in principle.

Unsurprisingly, then, there is a strong privacy response to this type of activity in all its manifestations, affecting our own. Trust in archival processing, so vital to the success of our policies and strategies in this area, requires the same level of understanding and transparency that governments are accused of failing to engender in their eGovernment implementations.[34] The problems multiply when scepticism about limitations to inter- and intra- government data sharing is added to the picture. In the current security conscious environment, this can only continue. The archival profession has to formulate strategies for the building of trust in its own processing, matching and sharing of personal information within public records regimes and without. This

[32] A further point is to observe that theoretical models such as the records continuum, unlike the lifecycle model, are not easily replicated in juridical instruments. This is another wider issue: the relationship of archival theory and practice (too wide an issue for proper consideration in a report such as this).

[33] This may imply a more complex articulation or at least implementation of the ATF requirements. There are likely to be a multiplicity of identifiers, and conformance with the requirement is likely to be as much about managing these robustly as adhering to them literally.

[34] Todd (2006, FN 46) cites J. A. Taylor, Mirian Lips and Joe Organ, "Freedom with Information: Electronic Government, Information Intensity and Challenges to Citizenship," paper presented at the *House of Commons Public Administration Committee FOI Workshop, University of Durham, April 2005*. Further analysis of the UK political scientific research cited in Todd (2006) is being published at the time of writing in *The Glass Consumer: Life in a Surveillance Society*, Susanne Lace, ed. (Policy Press / National Consumer Council, 2005).

will ensure that the debate about the placement of the public records part of the profession within or to some degree detached from the bureaucracy needs to be continued and brought to some sort of settlement.

There is a converse—almost a *perverse*—effect from the politically charged citizen identifier issue: if the single identifier is the only attribute used to tie disparate documents together in the business process and record creation environment, its absence destroys the integrity of the assembly. It will likely be the only linkage to the human readable, identifiable data of personal name and so on. This means that the question of archival access to such identifiers, at least as they refer to historical digital archives taken into custody, is essential if this vital contextualisation is to be preserved linked persistently and inextricably to the rest of the record. Archivists have to make representation to policymakers on this issue or the context, identity and authenticity of the archives from today and the future will be irrevocably compromised.

Presentation of incomplete archives

In addition, even if the juridical and theoretical issues examined in the research can be resolved, there is a further perceptual problem with the presentation of incomplete archives, especially over the internet and particularly if this is to become the normal interface with digital archives; even more so if this is to become the major vehicle for FOI releases.

This problem is an accumulation of the digital trust, user experience, general level of decontextualisation and limitation of secondary purpose use issues already mentioned. A more mature understanding clearly requires fostering between different disciplines: the conceptual analyses conducted in Domain 2 show that our scientist colleague allies do not have precisely the same concerns as archivists. Some of these issues should be taken forward by InterPARES 3 to assist with cementing such alliances.

8. InterPARES 2 Case Study Research

Case study research questions

Of the twenty-three research questions used to gather information from records creators within the InterPARES 2 case studies, the most directly relevant to this subject are:

20. *To what extent do policies, procedures and standards currently control records creation, maintenance, preservation and use in the context of the creator's activity? Do these policies, procedures and standards need to be modified or augmented?*

21. *What legal, moral (e.g., control over artistic expression) or ethical obligations, concerns or issues exist regarding the creation, maintenance, preservation and use of the records in the context of the creator's activity?*

Other data to support the analysis of the information policy issues being studied here will occur in the general characterisation of the case study in its introductory description and incidentally in a number of other of the research questions. For example: with some case studies it may be

revealed by the detailed description of the digital entities (questions 2, 3 and 4) or more detailed issues such as descriptive standards (questions 4, 7 10 and many others).

Much of the policy level analysis though will be involved in working out how these issues from creator based case studies might map forward into the preservation domain. Some of this, as will be seen, is hypothetical projection. Where it meets the higher-level policy analysis derived from different policy data collection techniques will be discussed in the next section.

The case studies

Case study coverage with privacy implications is currently limited to Focuses 1 and 3. There are no social or life science case studies present in the research data that would have integrated examples of the policy trends from these sectors. Hypothetical appraisal scenarios pushed forward from these might enable validation of other study at the legislative level. This has not, to date, been attempted: it may be a task to consider for the final stages of the research as Domain 3 looks at appraisal and preservation.

Revenue On-Line Service, Ireland ('ROS')

ROS is a complex online e-Government transactional system. Although juridically it contains public records—citizens use the service to declare their tax liabilities to the tax authorities—as with so many of the electronic record creating environments observed in InterPARES 1, little thought has apparently gone into the management and preservation of the records, nor even into defining what they actually might be and where the reside.

In keeping with the environments being studied in InterPARES 2, ROS is highly interactive between the citizen using Web forms at the Web interface and then backward from there to a series of databases at the back end. ROS also interacts with users' banks for the making of payments. There is an apparent blurring of documentary forms comprising documents, XML messaging, databases. This scenario is not easily understood in terms of InterPARES 1 type entities.

Diplomatic analysis and record identity

In such an environment, there may be many entities that might qualify for record status.[35] All are currently treated by creating organisation as 'data,' but juridically they are clearly records.[36] The current regime for the retention of the 'data' is plainly inadequate for current business needs: the organisation hopes that limitation periods will allow purging of 'data' before the system's capacity is reached. There was no provision for any other archiving routines—for any purpose—observed in the case study.

The diplomatic analysis undertaken for this case study notes that whilst the entities studied (the digital certificates, the tax forms and the debit instruction forms) each met all of the record

[35] It may be that this level of complexity and its multiple possibilities for record candidature right across the ROS—as opposed to confined to the three entities studied—might be seen as analogous with such scenarios as the Australian HealthCONNECT system studied from an archival perspective by Livia Iacovino in her 2004 article, "Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and HealthConnect," *Journal of Law and Medicine* [Australia] 12(1): 40-59. As proposed in this research, the continuum model seems particularly well adapted to comprehending the complexity of such systems.

[36] However, only the Public Key Infrastructure and related aspects of the front end were considered in the case study.

requirements identified by InterPARES 1, the severe problems with the preservation of the entities that might be expected from the foregoing was confirmed. Specifically: there are both technical and juridical barriers to the preservation of the records.

The use of asymmetrical Public Key Infrastructure ('PKI') to create and maintain digital certificates is the only apparent manifestation of the identity of the originator of the record (though not its creator, which is ROS itself). As noted in InterPARES 1, this presents a preservation challenge that may be insuperable without early intervention, although it is vitiated to a degree not found to be common in the study as the public authority rather than a more ephemeral third party is the signature provider. There may also be a secondary effect on the identity of the record: not in this case the most serious threat posed by the inability to preserve the personal identifier of the creator of the record, but the apparent arrangement of the records within the aggregation by personal name or other personal identifier derived from or representing the PKI algorithm. This applies equally to the digital certificate, the tax form and possibly also the payment instruction.

From both the case study report and the diplomatic analysis, it appears that the problem can be traced back to the use of asymmetrical PKI (an unpreservable technology in the long term in itself) to manifest the identity of the individual in the other two entities qualifying as records. See the Data matching and eGovernment identifiers subsection in section 7 for a discussion of the policy issues.

Authentication and identity issues

Because of the comprehensive implementation of the EU eCommerce Directive in Ireland, with both standard and advanced (non-repudiable) digital signatures and its enthusiastic take up by the Revenue Service, ROS makes extensive use of asymmetrical digital authentication techniques (PKI) and thus of cryptography. The implications in terms of preservation have been well rehearsed in previous InterPARES research and the discussion above adds additional concerns to the effects of this on personal information and the management of individual and record identity / authenticity.

InterPARES 2 privacy analysis

This must remain hypothetical owing to the unlikelihood of the records being appraised as for archival preservation, but even the reasons why may be instructive in the context of this report. The tax records relating to individuals are simply considered too personal to be transferred to a permanent archive under the EU Directive EC/95/46: this would represent a disproportionate invasion of privacy. In addition, the Revenue Commissioners have a duty of confidentiality to individual Irish citizens that might subsist until at least their deaths.

Whilst in theory, the workings of the archival exemptions in the *Irish Data Protection Act* with the *National Archives of Ireland Act* could claim a compatible historical purpose and some *vires* for the Archives preserving the records, this is highly unlikely to happen.[37] As noted in section 5, it is not clear whether exemptions for historical purposes in the European Union can override the

[37] And, as noted in the final paragraph of the ROS diplomatic analysis (see http://www.interpares.org/display_file.cfm?doc=ip2_cs20_diplomatic_analysis.pdf), in theory the authorisation of the destruction of the records is a requirement of the *National Archives Act*.

fair processing principles of the Directive. The National Archives is unlikely to change its selection policy to include such records. Even if it did and braved the storm that might ensue, it would not be able to release the records until it was sure the data subjects were deceased. Under Human Rights, it may be that the privacy of direct descendants could be affected (see above).

Legacoop, Bologna, Italy[38]

Legacoop is a self-governing cooperative association in the tradition of the north Italian left. Its recreation as a Web-based community as part of its core business functions shows that it has been enabled in new ways by the digital environment. Whilst self-governing, for the purposes of categorisation within InterPARES, the case study is associated with the eGovernment focus (Focus 3): it is neither for profit, not artistic, nor scientific, nor for common good.

The Web site is partly in the public domain of the World Wide Web and partly confined to Legacoop members. These latter password protected areas contain personal information posted by members of the community to realise very immediate benefits to themselves and other members: job applications, CVs, advertisements for consultancy services, etc.

The main interest in the current content of the site is the facilitation of the community and the attraction of new members through its public Web presence. From an archival perspective, the preservation interest would centre on the community's own sense of identity and its placement within the Commune of Bologna, but Domain 3 may also associate wider interest in associated Italian Co-operative organisations. The Community itself is associated with the Bolognese social economy archive centre as an active participant, which led to its collaboration with InterPARES.

The final case study report notes the need for more formal procedures for the management of the Web site if its preservation is to be facilitated.[39] In particular, the answer to research question 4.1 is instructive:

(a) To what extent do policies, procedures and standards currently control records creation, maintenance, preservation and use in each policy area?
(b) Do these policies, procedures and standards need to be modified or augmented?

A number of threads apparent in the discussion of the policy environment of contemporary privacy above are discussed by the Report in answer to this question: identification of the record(s), integrity reliability and authenticity, juridical requirements for use of authentication technologies. There is scant data in the report that focuses on privacy and what follows is an attempt to extract according to those themes and establish a privacy angle.

[38] The privacy analysis offered here is based on research data abstracted from the final case study report by lead investigator Maria Guercio (see http://www.interpares.org/display_file.cfm?doc=ip2_cs25_final_report.pdf).
[39] The site shows the phenomenon observed in the first phase of InterPARES: records created in electronic systems with inadequate controls compared to the requirements set forth by the Authenticity Task Force. See Authenticity Task Force (2002), "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records" in *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Italy: Archilab, 2005), 204–219. Online reprint available at http://www.interpares.org/book/interpares_book_k_app02.pdf.

Identification of the records, authenticity and authentication[40]

The results of the diplomatic analysis of this case study were not available when this report was drafted, but can be inspected at: Carolyn Petrie (2006), "InterPARES 2 Project - Case Study 25 Diplomatic Analysis: Legacoop of Bologna Web Site."[41]

Juridically, the Web site may in some respects be caught as for the documents of a private company: Italian civil law is very precise as respects requirements for authentication, enacted under the EU e-commerce Directive and relying on third party provision owing to single market regulations.[42] Certain specific categories of document require digital authentication in this juridical sense by the [private] legal entity. Compliance with the provisions—if they impact on the Web site[43]—will have to take note of the concerns expressed below.

Privacy analysis[44]

In this case study, the management of privacy is not particularly demanding to analyse. The site is 'interactive' only to the extent that it uses Web forms and different users have slightly different views of it. The personal information content is mostly concentrated in discrete areas, the management of which is facilitated by the hierarchical nature of the Web site. This structuring by the records creators neatly differentiates the personal information from the rest. Consequently, access administration in an archival domain (amounting to incremental release as more information reduces in sensitivity) would be straightforward.

Privacy requirements will impact on the appraisal of records in EU jurisdictions, including Italy. Archival preservation of the Web site is clearly compatible with the business objectives of Legacoop and this definitely includes to the purpose for which Legacoop members submitted documents for posting to the site. Consent for this purpose can thus be inferred with complete confidence from this submission.

Thereafter, things get a little less clear-cut. Strictly speaking, historical purposes have to be identified by Legacoop prior to the business purposes for which they retain the personal data has expired, otherwise the organisation has no *vires* to continue to process [retain] it. It is a moot point whether identification of an historical purpose exonerates EU organisations from clarifying to data subjects that their personal information may be preserved (there is a legal duty for it to be protected from unrestricted access and use within the lifetime of the data subject). Although for InterPARES purposes this is an eGovernment case study, no archiving provisions in a public records regime here mean that this is the will of the legislative authority.

If it does not already do so, it is recommended that Legacoop has a public statement for its members on how it sees its cultural role so they are aware of the possibility of their personal

[40] See policy recommendation 4 in section 5.
[41] Available at http://www.interpares.org/display_file.cfm?doc=ip2_cs25_diplomatic_analysis.pdf.
[42] The outcome of the diplomatic analysis may inform whether this is in fact the case.
[43] After the drafting of this report, it was determined by the case study that the status of the Web site content as supporting records did not require the use of digital signatures. This might change if the site became transactional.
[44] The case study participants' response to the research question, "What legal, moral (e.g. control over artistic expression) or ethical obligations, concerns or issues exist regarding the creation, maintenance, preservation and use of the records in the context of the creator's activity?" reads "The creator has no obligations other than ethical ones relating to the correctness of what is available on the Web site." To the extent that some of the information is personal, the legal ethical and moral issues associated with privacy appear to have been downplayed.

information being preserved. Depending on the outcome of the consultation process that this may involve and any juridical requirement in this area, it is recommended that an opt-out or even a conscious opt-in is instituted and trust in this process honoured in the observance

The remaining points that can be drawn out of the case study are concerned with the interplay between the technical measures taken to protect personal information in the current business environment of the Legacoop and how these might affect preservation. The presence of cryptographic techniques to protect personal information is a distinct barrier to preservation of parts of the site.[45]

The impact of these on those documents subject to digital signatures as providing the identity of the participants and—potentially—the identity of the records is clearly problematic unless the signatures can be rendered inoperative as content may be passed to archival custody. There is insufficient technical detail in the case study to evaluate whether the use of password protection is at the level of the operating system (where cryptography may also jeopardise access to the documents) or at the application level through access controls applied through the content management system. The latter would be preferable from a preservation point of view if consent were forthcoming to archive the content concerned and would be dependent on a viable way of extracting the content and description and transferring it to an archival platform.

Focus 1 (collaborative Artistic activities) case studies privacy issues

In general, the revelation of self inherent in the expression and communication of many performance art forms—including digital ones—would be covered by the normal exception to privacy protection where the performer had themselves put the information into the public domain. The disclosure of information about others has always been in the background of this, but virtual, collaborate and distributed communities may produce privacy case law of this new kind in the future.

- At the level of all the individuals involved, establishing *definitively* the consent of *all* the participants to the continued retention of their personal information and its reconstruction by the archives is likely to be problematic, yet is in theory required.

- Yet, there is an interesting aspect to the privacy issues present in this scenario that is at present non-juridical: privacy usually relates in law to natural persons or organic groupings such as the family, as has been discussed previously in this report. The recreation of some interactive art collaborations may imply a perceived invasion of privacy of a grouping that only existed for the purposes of the performance.[46]

This is at present a hypothetical issue, though it should be passed at this point to Domain 3 as it considers appraisal and preservation strategies for the Focus 1 case studies.

[45] This was very much an interim suggestion offered to Domain 3 at the time of writing for their consideration and is hypothetical given the inconclusive nature of the appraisal discussion above.
[46] See footnote 10 to policy recommendation 1 in section 5.

Appendix 1: Abstracted policy recommendations (from Section 5)

1. No single definition of privacy; need to monitor both statute and case law.

2. Legislative frameworks need *explicitly* to make adequate provision for archival activities.

    a. Many legislative frameworks require revision and greater integration of issues of privacy, Freedom of Information, archival access. This may be done through the articulation of a clear archival exemption that recognises clearly the need to respect the integrity, identity and authenticity of digital records. For example, if there are general duties to update "data," it must be clear beyond doubt that these do not apply to the archives. Such an exemption may be tied to purposes or institutions but the implications of this must be thought through in terms of the jurisdiction's archives model.

    b. If the archival exemption is articulated in terms of purposes compatible with the original purpose of the data being collected and used, a wide rather than narrow definition of 'compatible [archival] purposes' is preferable. Similarly recognition is required that some archival 'processing' of personal information (e.g., preservation activities such as retention and migration) is of a lesser order of processing than taking business decisions affecting the individual to whom the information relates. It may be preferable to define these as concepts in the law distinct from 'processing' to facilitate this.

    c. Many archival laws and regulations have lagged behind innovation in the privacy area and there is ambiguity about primacy of provisions.

3. Integration of ethical issues in archival access is required, especially by the use of ethical researcher codes. Scope for these has been squeezed and may now have to deal with extremely difficult areas.

4. There is a blurring of the public / private by use of intermediaries / contracting out by governments, with profound and worrying consequences.

5. Additional urgency is added to that identified in the InterPARES1 Appraisal Task Force reports for the early identification of archives of historical value *and their transfer to archival custody.*

6. Archival policies and practices must be sensitive to the difficulties of balancing the ambiguous position of the public archives.

7. Contribution of the archives to building Digital *Trust.*