Power, Identity, Integrity, Authenticity, and the Archives: A Comparative Study of the Application of Archival Methodologies to Contemporary Privacy*

MALCOLM TODD

RÉSUMÉ Le droit au domaine privé (« *privacy* ») occupe une place proéminente dans la gestion des archives et par conséquent dans la littérature. Comme archivistes, nous avons un rôle de confiance afin de déterminer l'accès aux archives dont nous avons la garde. Ceci est une zone qui, en raison de la marche progressive de la technologie, se développe rapidement dans son administration, même si son but ultime est constant : assurer un accès approprié au patrimoine documentaire. Ce texte tente de faire le lien entre les développements dans ce champ identifiés lors de travaux effectués grâce au projet InterPARES et les questions de méthodologie archivistique et même la théorie. Les tendances en jurisprudence et en politique montrent que même si nous pouvons nous attendre à ce que notre gestion de l'accès soit jugée, il y a d'autres défis aussi fondamentaux qui doivent être affrontés. La mondialisation du commerce, le partage de données gouvernementales et la jurisprudence signifient que même là où la réglementation stable et équitable du droit au domaine privé a été mise en place – comme elle semble l'avoir été au Canada – il reste qu'il y a des menaces et des défis graves à cet accommodement. L'élément du consentement dans le contrat actuel entre le citoyen et les archives devra peut-être être réétudié plus tôt que prévu. Ces défis sont examinés tels qu'ils se rapportent aux méthodologies professionnelles établies. Enfin, en apportant à cette discussion le postmodernisme philosophique de Jacques Derrida et les approches archivistiques postmodernes tel qu'exemplifié par le point de vue du continuum, la définition, le potentiel et les limites du droit au domaine privé comme proposition archivistique postmoderne sont considérés.

* A related paper co-authored with Livia Iacovino of Monash University was presented to the 2004 ACA Conference under the title: "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." This was part of a panel presentation on moral rights by the InterPARES policy team under the 2004 ACA theme of Ethics and Accountability in the archival sphere. A revised version of this paper, "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" is pending publication in *Archival Science* and is referred to here as "Iacovino and Todd." The author is very grateful to Livia Iacovino for her collaboration on these papers, to Frank Upward for his comment on the use of the term "postmodern" and to the editors and their reviewers for their apposite comments on the draft. The subsisting shortcomings remain the author's own. The opinions expressed in the paper published here are to be taken as the official views neither of The National Archives, nor Her Majesty's Government.

ABSTRACT Privacy has a prominent place in the management of archives and consequently in the literature. As archivists, we have a trusted role in determining access to archives in our care. This is an area that, owing to the onward march of technology, develops rapidly in its administration even if the overall aim is constant: ensuring appropriate access to documentary heritage. This paper attempts to link developments in this area identified in previous work under the auspices of the InterPARES project to issues of archival methodology and even to theory. Trends in jurisprudence and politics mean that although we can expect still to be judged on our management of access, there are other, equally fundamental challenges to be addressed. Globalization of commerce, governmental data sharing, and jurisprudence means that even where a stable and balanced regulation of privacy has been achieved – as it seems to have been in Canada – there are deep-seated threats and challenges to this settlement. The element of consent in the current compact between citizens and the archives may need to be revisited sooner rather than later. These challenges are discussed as they relate to established professional methodologies. Finally, by bringing to bear the philosophical postmodernism of Jacques Derrida and postmodern archival approaches as exemplified by the continuum viewpoint, consideration is given to the definition, potential, and limitations of privacy as a postmodern archival proposition.

Public policy agendas aimed at protecting the privacy of individuals demand a response from the archival profession if we are to remain the guardians of, and continue to receive, archives containing personal data. In the course of a comparative study of contemporary privacy regimes, Iacovino and Todd found that the response to global terror and freedom of information (FOI) have combined with concerns about electronic government initiatives to tighten privacy regulation in many jurisdictions. Exceptions are the far weaker protections available for privacy in the United States and in the "for profit" sectors rather more widely. Even these qualifications have a tendency to present problems for the archival mission in an increasingly global networked environment.

For archivists, the main challenges come from very prosaic roots. To begin, we now have to manage privacy at the sub-record level. Many issues in the past could be managed at a higher level, whether the entire record, aggregations of records or organizational fonds. Considering the remit of InterPARES2 to address the requirements for authenticity arising from records created in dynamic, experiential, or interactive systems[1] in the arts, sciences, and e-Government, this is challenging indeed. The records may not now be manifest in a coherent, stable form and the personal information within and/or linked to them may be in further disarray. The availability of records contain-

1 "Experiential" systems is a category InterPARES2 has taken from Clifford Lynch, "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust," in Council on Library and Information Resources, "Authenticity in a Digital Environment" (Washington, May 2000), available at <http://www.clir.org/pubs/reports/pub92/contents.html>. See also <http://www.cni.org/> (both accessed 14 March 2006). Its exact meaning has been a point of lively debate within InterPARES2 since, according to the findings of InterPARES1, all electronic records are dependent on rendering to an interface providing an experience to the viewer and therefore in a sense "experiential." See footnote 30.

ing personal data for appraisal and our – or the creator's – right to hold and preserve them may themselves be subject to challenge: we cannot preserve what we have not taken into custody.[2]

This is a break with the past, when public bodies, whether records creators or archives, could generally retain records containing personal information under generous "blanket" provisions with an impunity derived from restrictions on access (except in some cases for the data subject). These could derive from general security or "sunset" clauses such as those in many statutory archival regimes. Provided the records were protected from unauthorized access for the period specified or some other appropriate and defensible period, archival institutions could look forward to releasing rich archival resources to public use. This reinforced, or at least did not contradict, the maintenance of the integrity of the archives. Giving data subjects or third parties access and/or complying with duties to correct and/or erase personal data turns this on its head. Jurisprudence spreading from the European Union calls into question the right to retain personal information under some circumstances.[3] The exact extent may only emerge through case law. In addition, there is a tendency to narrow the definition of what are acceptable secondary purposes, especially where this has not been clearly articulated for our community. The consequences of this are profound. Accordingly, it makes sense to focus on two main problematic areas: the respective threats to archive *building* and to archive *integrity*.

In the first case, technological innovation manifest in e-Government and globalization have "upped the ante" considerably in the past few years, leading to unprecedented concern about the "surveillance society," data sharing, matching, and unauthorized disclosure. This means that the territory on which this argument will be made is not solely the accustomed professional one about access to archives containing personal information, nor can it continue to observe a simple "public" versus "private" sector split. In the public sector, both federal and provincial Canadian legislation is characterized by a tight

2 Equally, many public institutions also have legal duties to preserve archives containing information that cannot normally be released, such as obscene, depraved (likely to deprave), inciting to hatred, blasphemous, seditious, libellous, or other material.

3 Under section 29 of the Directive 95/46 EC, the transmission of personal data from the European Union is only permitted if the receiving environment has either a legal or contractual framework deemed to have equivalent protection. This has forced other jurisdictions or multinational companies to respond in law – as witnessed by the *Personal Information Protection and Electronic Documents Act* (2000) in Canada (PIPEDA) – or through contractual arrangements. See Tim Cook, "Archives and Privacy in a Wired World: the Impact of the Personal Information Act (Bill C-6) on Archives," *Archivaria* 53 (Spring 2002), pp. 94–114; and Iacovino and Todd. Yet, as we shall see, the EC Directive is a symptom rather than the cause of the underlying jurisprudence causing an expanding portfolio of moral rights to be enshrined in law.

integration between access to information and privacy legislation.[4] Measures are frequently passed in tandem, clear articulation of the archival exemption(s) and even clauses clarifying for the avoidance of doubt the primacy of record integrity that archivists in other jurisdictions might envy. Tim Cook alerted readers in *Archivaria* 53 to the partial nature of the success of the archival lobby in influencing the provisions of PIPEDA. Here record integrity is less certain and the ability to appraise and acquire private archives much less certain. More worrying still are the apparent views of the Privacy Commissioner with regard to census data, and not solely with regard to the 1991 census.[5]

Other archival commentators agree that the ground of the argument has broadened in this way and several will be heard from later. Heather MacNeil's most recent paper on the subject, "Privacy, Liberty and Democracy,"[6] argues that more participation from archivists is required, based on their unique perspective on the balance between the right to privacy and society's right to knowledge:

> Judging from the dearth of substantial discussion in the archival literature, however, it is fair to conclude that archivists are generally disinclined to participate in such debates. To the limited extent that they do participate it appears that, while they do not dispute the significance of individual rights to privacy, they are more inclined to publicly promote the importance and value of increased accessibility to archival holdings.[7]

There is a distinct threat of further development of the privacy agenda that could lead to the recognition in law of moral rights beyond those that are compatible with our role. This raises important professional and political ques-

4 This is witnessed by the common practice of referring to the federal *Privacy Act* and the *Access to Information Act*, both from 1982, collectively as "ATIP." A provincial example of the same tendency is provided by 1997 Manitoba legislation, the *Freedom of Information and Protection of Privacy Act* (FOIPPA). Here, the parliamentary drafting expounds at some length the sort of issue of importance to the profession, and in a clear, accessible fashion alien to many Westminster systems. See FOIPPA, ss. 38–40 on the duty to correct by means of annotation or s. 43(v) on transfer to "the Archives of Manitoba or to the archives of the public body for records management or archival purposes." FOIPPA, accessed at <http://web2.gov.mb.ca> (January 2006).

5 See Cook, "Archives and Privacy." Summarizing this article broadly, the problematic areas remaining are recognition of historical purposes – "scholarly" or otherwise – as distinct from journalistic, artistic, or literary, archival purposes as distinct from "scholarly," processing by solely archival institutions, an additional compatibility provision for archival processing and the lack of de-encryption regulations. The successes of the archival witnesses were with respect to closure periods and the articulation of their arguments.

6 Heather MacNeil, "Privacy, Liberty and Democracy," in Menzi Behrnd-Klodt and Peter Wosh, eds., *Privacy and Confidentiality Reader: Archivists and Archival Records* (Chicago, 2005), pp. 67–81.

7 Ibid., p. 68.

tions about the roles of archives and archivists. It boils down to whether we, in a plural democratic society, have the public's mandate to maintain what we see as our mission. To put it another way: is there a public interest in the archived collective memory that is higher than some of the mantras of the privacy lobby and how is that argument to be won whilst perhaps other, less inimical privacy concerns can be satisfied? Effective archival exemptions or the recognition of the compatibility of (our) purpose by both legislators and the citizen will need to adapt to this dynamic. These are our profession's strategic privacy priorities, followed by ethical dimensions in researcher access in third place. To work out how we might promote this requires some conscious consideration of how archival exemptions to privacy protection have been conceived, framed, and meshed with our own professional and policy instruments. All this merely so we can be sure that we can continue to *take archives into custody.*

The challenge to the *integrity* of the archives continues to be based on the generic requirement to destroy, expunge, or "correct" personal data that is inaccurate, out of date, or no longer required for the purpose for which it was collected.[8] Clearly we have a long-recognized need for effective exemption in this area also, but it is one that requires some thought at this juncture and for much the same reasons. *What, exactly* are we seeking to preserve and arbitrate access to? To achieve this, and in common with other policy issues considered in InterPARES2, we shall have to address concerns in juridical systems that are explicitly "about" privacy and personal data and neither understood nor articulated in archival terms.[9] This has been approached by mapping forward some of the findings of the first phase of the InterPARES project and engaging with some additional archival literature to distill how personal data participates in the authentic archive. Some of this literature, honouring the theme of "archives and power" is from markedly different traditions.

This paper will submit that the application of continuum thinking to this archival problem is also a postmodern and relativist argument. This contrasts with the traditional playing out of the life cycle in those statutory archives regimes where creator and preserver are part of the same bureaucracy. This can with some justice be characterized as a positivist argument. Irrespective of

8 As a minor pendant to this point, there is the tendency for some *Freedom of Information Act* (FOIA) regimes to promote access to partial records, which may undermine the perceived importance of integrity.

9 A series of five policy studies have been conducted, contributing to a policy framework and principles. The framework is designed to overcome the identified barriers to the preservation of authentic records as understood by the intellectual framework of the project. The studies found that most juridical instruments, even archival legislation, talk about records in terms of physical custody, evidence procedures, etc. Privacy thus shares with authenticity and archives legislation the tendency to speak of physical entities that an archivist could consider a conceptual record ("extracts" from a public register, case files, "data," etc.).

the stance of the individual archivist, though, these dimensions of the subject require a general attention from the profession they do not seem to be receiving.[10] This paper attempts to demonstrate that the professional discourse greatly enriches the consideration of the privacy issue. To sum up "the problem" considered by this paper: it is necessary for the profession to wake up to the fundamental challenges posed by privacy. Left unchecked, we may be jeopardizing the survival of large areas of our current professional activity.

InterPARES Issues and Recommendations

This paper will look at two main areas of concern emerging from InterPARES research and push them into the discussion areas outlined above. The first are the privacy policy recommendations emerging from the findings of Iacovino and Todd due for publication shortly in *Archival Science*[11]:

1. the need for a broad rather than a narrow determination of the compatibility of purposes, recognizing archival purposes specifically[12];
2. the need to [re-]integrate archival legislation into access regimes for public records [including where necessary FOI regimes] where this is not/has ceased to be clear[13];
3. the added urgency given to early appraisal decisions;
4. the need for e-Government implementation to guard against pervasive decontextualization of records, for example by using only data matching identifiers;
5. the need for the development of private sector privacy regulation in public policy, especially in the United States but also in other extra-EU jurisdictions such as Canada and Australia where there is immaturity apparent in this area;
6. the enhanced need for the unequivocal consent by private records depositors so they can be deemed to have placed their personal archives in the public domain of their own volition;

10 Though it certainly is in the sights of many of the colleagues whose work is gratefully referenced here.

11 A policy report drawing on this work, the present paper, and other research will be published at the completion of the project in 2006–2007.

12 European enactments of the Data Protection Directive reflected widely different articulation of the archival exemption to the general principle of personal data only being used for the purpose for which it was collected and not retained further. The extent to which the archival purpose is explicitly and effectively provided for was also noted, paralleling in many respects Tim Cook's account of the PIPEDA debates. Civil law jurisdictions such as the Italian and common law such as the Irish have categoric exemptions (the latter only appearing to apply to records caught by the *National Archives Act*), others far less so.

13 A discrete related study of archives legislation is continuing within the InterPARES project and comparisons between the two policy areas will be established in the final Policy Report in 2006–2007.

7. the need to ensure that duties to correct inaccurate information do not interfere with the integrity of records [i.e., they should operate by annotation rather than expungement];
8. the need to recognize the moral dimension in privacy regulatory frameworks; and
9. the need to promote archival and researcher access codes into the legislative framework, as has been achieved in Italy[14] (and to an extent in Canada[15]).

It is possible that, globally, a number of distinct pragmatic strategies will be required to support these international recommendations. For example, the social science and scientific research communities have a common purpose with our profession on these issues, up to a point. Similarly political science might agree that stressing the fundamental role of archives in the protection of human rights may be every bit as significant as privacy. They are unlikely, though, to appreciate immediately the theoretical dimensions of our professional concerns about privacy. Canadian colleagues will note that in their jurisdiction(s) some of these recommendations have already been addressed. This puts the Canadian profession and its mission at an advantage over many of its peers. Iacovino and Todd noted particularly a tight integration of privacy and FOIA regimes and the advantages of the "total archives" concept in integrating the regimes for the collection of public and private archives. Even in Canada, this hardly gives grounds for complacency. What is less obvious is any awareness across the professional community of the complexity of consent issues likely to challenge the current settlement. There are tectonic forces in play: an international jurisprudence exists and continues to develop in this area, and is driven by concern about privacy in the global digital environment.

The second group of core InterPARES issues is the nature of the participation of personal information in the archives, its relationship to authenticity, and the maintenance of the integrity and identity of the record.[16] The identity both

14 *Codice di Deontologia e di Buona Condotta per I Trattamenti di Dati Personali per Scopi Storici*, 28 February 2001, published in the *Gazetta Ufficiale, Serie Generale*, n. 8 of 5 April 2001. This paper does not concern itself further with the issues of the arbitration of access to archival records, except incidentally.

15 Witnessed by the attachment to PIPEDA of the Canadian Standards Association's *Model Code for the Protection of Personal Information* and such regulation of researcher access as found in the Manitoba *Personal Health Information Act*, ss. 22–24 (or the FOIPPA already cited, ss. 44–48).

16 This section discusses the privacy issues arising with structured personal information about either the persons concurring in the formation of the record or participating in the action it records. Issues of "incidental" or unstructured personal information in the content of the record are discussed in the final sections on participation and consent. Personal information in the first category is a *sine qua non* of any conceptual notion of documentary form.

of individuals and of records are familiar issues from the wider literature. The *Authenticity Task Force Report* of the first phase of the InterPARES project[17] proposed two sets of requirements to support authenticity as defined by the archival and diplomatic science methodologies of the project: the *benchmark* requirements to support the presumption of authenticity of archives, and the *baseline* requirements to support the certification of copies of records, by an archival institution, the project having established in a theoretical sense that there was no longer any meaningful sense of an "original" record. The conceptual framework of authenticity includes the following statement:

> The identity of a record refers to the distinguishing character of a record, that is, the attributes of a record that uniquely characterise it and distinguish it from other records. From an archival-diplomatic perspective, such attributes include: the names of the persons concurring in its formation (i.e. its author, addressee, writer, and originator[18]) ...

Among the more detailed record identity requirements designed to fulfil this, the names of the persons concurring in the formation of the record are of cardinal importance, witnessed by the statement: "... the value of the following attributes are explicitly expressed and inextricably linked to every record."[19]

The requirements also cumulate: the extent and number met increases proportionally the presumption of authenticity. Whilst some of the requirements could be said to introduce an element of relativism into the judgement of authenticity, it is difficult to see how non-satisfaction of Requirement A.1.a.i, the identity of the record, could do anything other than undermine the presumption of authenticity.[20] Viewing the issue of privacy from within the intellectual framework of the InterPARES project, it is possible to observe that it is essential for the policy objectives outlined above to be addressed for the presumption of authenticity to be satisfied. One could go further and note that whilst *all* established archival methodologies must concern themselves with

17 In Luciana Duranti, ed., *The Long Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project* (San Miniato, 2005), pp. 20–66.

18 Ibid., p. 21. It clearly shows a combination of diplomatic and archival thinking and terminology, some of which will be returned to in this paper.

19 See Duranti, ed., *Long Term Preservation*, specifically Requirement A.1.a.i, *Identity of the record*.

20 Within the conceptual framework articulated by InterPARES1, the only arbitration of the authenticity of a record prior to its transfer to archival custody is the reliance on it by the creator in the course of business; these requirements are aimed precisely and solely at supporting the presumption of authenticity once custody has been transferred (benchmark requirements) and the subsequent production of authentic copies (baseline requirements). This is a viewpoint imposed by the methodology of the project. Taken to an extreme, this could introduce a conceptual disconnect between the management of personal data contained within the records before and after transfer, were it not for the diplomatic insistence on the identification of the responsible actors.

the integrity of the archives, the elevation of particular requirements to fundamental status based on diplomatic theory, and/or their presence in a typology of authenticity, means that there is a particularly acute difficulty in accepting archives where these characteristics are not present. The point here is mainly one of anonymization: if personal information has had to be removed, fundamental characteristics of the archives are compromised. This is an issue both of deidentification and decontextualization and is likely to be particularly acute in the characteristics of the participants in the records creation process.

There will be more discussion of concepts and techniques derived from the diplomatic school later in this paper. For now, a very general further point is offered and it does not require a convinced theoretical viewpoint to subscribe to it: *viz*. the demonstration of an authenticity that can only derive from the primary purpose and its documentary form acts as a "pivot" on which all secondary archival purposes of the record[s] must depend.[21] After all, it is only in understanding its provenance that we can judge whether it can bear any witness to these other purposes. This is based, *inter alia*, on the identification of the participants in the record-making process and their competence in terms of their contemporaneity with the recorded act, their official position, and so on.[22]

The outcomes of the UBC Project[23] that preceded InterPARES could be described as proposing a typology based on archival diplomatics for the authenticity of electronic documents considered as discrete items. This necessitates specific archival controls to be imposed in the creating environment. Similarly, the InterPARES1 *Authenticity Task Force Report* distills its contextualization demands down to the issue of archival description (being undertaken in the current phase of the research), relationships of records with each other, and the observation that there was worrying inconsistency apparent in the project's case studies surrounding how identity attributes were captured and expressed.[24] Other traditions have tended instead to stress a cumulative, circumstantial effect of record aggregations and description at various levels to support both the presumption of authenticity and the integrity of individual

21 The following paragraph touches on the document-based notion of provenance derived from diplomatics in contrast to the aggregation-based one from archival science.

22 For example, medieval historians have constructed many judgements of political power on the lists of witnesses attesting and applying their identifying marks to (mainly ecclesiastical) charters.

23 Luciana Duranti, Terry Eastwood, and Heather MacNeil, *Preservation of the Integrity of Electronic Records* (Dordrecht, 2002). The influence of this on the requirements of the Joint Information Technology Committee of the US Department of Defense standard for records management applications (DoD 5015) is well known.

24 The Task Force worried about this: "in the absence of a precise and explicit statement of the basic facts concerning a record's identity and integrity, it will be necessary for the preserver to acquire enormous, and otherwise unnecessary, quantities of data and documentation simply to establish those facts." Duranti, Eastwood, and MacNeil, *Preservation of the Integrity*, p. 8.

records as well as the fonds. It is worth noting that this too has tended to encourage similar controls on records creation and management, but with significant differences such as a more liberal use of metadata.

Reconciling the challenge of context contained within the privacy objectives outlined at the start of this paper now requires consideration of the record creation environments encountered in dynamic, experiential, and interactive systems studied in InterPARES2. Unfortunately, at the time of writing, there is little emerging case study data with privacy issues to illustrate this in a compelling manner. It is possible, though, to hypothesize on some very significant issues at a policy level especially as they relate to e-Government.[25] A number of jurisdictions have policy proposals for the implementation of e-Government identifiers – often linked to public key digital signatures – with the intention that these be used as the principal means of identifying citizens in on-line transactions. This is particularly controversial in the United Kingdom through its linkage with identity cards: since the abolition of austerity food rationing in the 1950s, there has been no general requirement on the UK citizen to carry a definitive means of identification.[26] This means that the issue of e-Government identifiers has become mired in disputes about the proportionality of the official response to global terrorism and may be an early casualty of the reduced majority of the Blair administration after May 2005. Such identifiers have a somewhat ambiguous relationship with the privacy agenda. Heather MacNeil noted and expounded the privacy objections to data matching in the USA and Canada at that time, especially the concerns about the accuracy of the information being processed.[27] In her later paper,[28] she quotes a latter day metaphor of the panopticon to illustrate the type of scenario that is now closer than ever to realization:

> ... as we look at each kind of information gathering in isolation from the others, each may seem relatively benign. However, as each is put into practice its effect is to close

25 The quantity of privacy data in the twenty-six InterPARES2 case studies has been disappointing. Significant material has been identified in two of the e-Government identified studies: Revenue on-Line, Ireland, and Legacoop, Bologna. Courtesy of the research of a colleague, aspects of an instructive Australian example from a complex e-Government system design have been incorporated below.

26 It is slightly ironic that UK citizens remain obliged to use their passports to travel within the European Economic Area within which there is supposed to be free movement of people (because the UK is not a signatory to the cross-border freedom clauses of the Schengen Treaty). The civil liberties lobby's objection is to compulsory identification within the borders of the UK, as well as to the e-Government data matching it may facilitate.

27 Heather MacNeil, *Without Consent: The Ethics of Disclosing Personal Information in Public Archives* (Chicago, 1992), pp. 42–44 and 52–54.

28 MacNeil, "Privacy, Liberty, and Democracy," p. 72.

off yet another escape route from public access, so that when the whole complex is in place, its overall effect on privacy will be greater than the sum of the effects of the parts ... I call this whole complex ... the informational panopticon.[29]

What InterPARES2 case study data does indicate almost across the board is that in a dynamic, interactive or experiential computing environment, the data entities manifesting the records are fragmented, and the ability to render the records coherently can only be maintained by reassembling multiple digital components.[30] Whilst the common factor governing these associations may not always be personal information, across transactions and their aggregations they very often will be. Data matching of some sort is, then, a *sine qua non* of e-Government and many other aspects of the information society. The policy objective of using single e-Government personal identifiers to match and share data about individual citizens gives added urgency to the issue of trust.[31] At the same time, from the point of view of the security of personal data the presence of an identifier rather than the full personal information of an individual must be said to provide some protection for private individuals should a subset of the records fall into the wrong hands. Beyond that, the concerns not so much with the state's mal-intent as its (in-)competence noted by Heather MacNeil over a decade ago could potentially reach new heights if multiple e-Government transactions are to be processed in real time with little human intervention. Many governments are working to facilitate such a model of service delivery. Aside from the established debate about accuracy, the potential disconnect between the process experienced by the citizen and implemented through the technical infrastructure must raise further concerns about trust in the handling of personal data. For the archivist, unless the personal details of the participants are either made explicit when the records are captured or can be linked subsequently, there will be a general effect of decontextualization that will be very detrimental to the value – even as we have seen to the validity – of archival records. To address this, we shall either have to ensure the identity of the participant citizen is made explicit as a procedure in records creation or the passing of comprehensive registers of e-Government identifiers to archival custody. Either has far reaching consequences, with profound trust

29 Ibid., quoting Jeffrey H. Reiman, "Driving to the Panopticon: a Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer and High Technology Law Journal* 11 (1995), p. 34.

30 This builds on the finding of the first phase of the project that it was the ability to reproduce the record that could be preserved in authentic form across migration rather than the record in any other (physical) sense. It is hoped to publish the case studies underlying InterPARES2 at the end of the project in December 2006.

31 Archives themselves will not be innocent of this: scattered and individually innocuous references in archives to surviving individuals could – if we provide users with the means of compiling them – constitute an invasion of privacy and this may affect such things as the functionality of search engines we provide to open up digital collections.

and privacy protection issues, that we as a profession have barely begun to address. They will often be encountered along with the encryption problems caused by the use of asymmetrical digital signature technologies.

All modern archival exemptions from personal privacy protection measures have to contend with the general principle that personal data must otherwise be processed only insofar as it furthers the original purpose for which that data was collected.[32] The processing of large quantities of digital data by commercial and governmental entities in the early 1970s produced this privacy response. Except for giving access to archival records, these considerations only became a pressing archival issue once "the" archival record was acknowledged to be digital. There are two main instruments that can afford archives exemption from this principle: a general exemption for secondary purposes explicitly or implicitly including archival ones, or a recognition that by virtue of an enactment, constitutional nicety, or something else, archival purposes nest conveniently within the primary purpose.[33] Immediately, different power relationships can be observed. The first manifests a general recognition of the beneficial effects of archives on society. The second, normally only afforded to public archives, is often indistinguishable from other exemptions governments give themselves from privacy legislation. This can itself be subdivided. On the one hand, there is the public purpose of maintaining private archives. On the other is the scenario of a statutory public archives regime wherein the personal data integral to the archives is maintained for operational use or its movement from the current or semi-current phase of its life cycle is indistinct.[34] All these scenarios are likely to have the imprimatur of the legislature, though it may be doubtful they were closely scrutinized by legislators and the public.[35] Such privileges are unlikely to be accorded to private archives in the custody of non-public archival institutions. This may be less severe in Canada with its system of "total archives" than in some other jurisdictions, but is nonetheless worth noting.

Clear generic mappings are easily identified with the broad life cycle and continuum models of the archival process. Where a succession of differentiated "phases" in the life of a record are assumed, as in the life cycle model, the

32 See, for example, Chapter 2 of MacNeil, *Without Consent*, pp. 35–59.

33 Internationally, many different devices are used. The archival purpose can be linked to a more general "research" or "historical" purpose as in the UK. Some enactments distinguish according to whether the holding institution makes a profit. Others specify particular (normally national) archival institutions or legislation, as in the case of the *National Archives Act* in Ireland.

34 Parallel InterPARES2 research on archival legislation has noted other issues if records are not moved through their life cycle by juridical instrument, with detrimental effects on their preservation.

35 Governments themselves, in fact, enjoy generous exemptions from some aspects of data protection and privacy regulation in the interests of security, efficient running of the state, etc. For example, it is possible for the state to commit a criminal act in neither the UK nor Canada by infringing data protection/privacy provisions. See the UK *Data Protection Act,* 1998 s. 63; and MacNeil, *Without Consent*, pp. 48–49 on the Canadian *Privacy Act*.

essential privacy issues concern the moments of transition between them, provided the juridical system acknowledges the change in the personal information's purpose. This very often is the case. For example, archival exemptions in federal and provincial Canada are tied to a cessation of administrative action. Effectively the – by now – historical nature of the personal information within the record is acknowledged. The continuum viewpoint at this level sees many strands of a record's existence occurring concurrently, such as historical purposes from or even before its creation. Reconciling this process modelling issue with privacy protection is complex: it requires consideration of each facet with each phase.

Leaving aside for the time being the power and accountability dimensions of the records continuum, let us consider the extent to which privacy regulation is adapted to its rejection of a linear life cycle model.[36] The latter tends to assign distinct roles, rights, and responsibilities to records creator, archives, and researcher. The "default" position of personal data only being used for its primary purpose and archives' need for an effective exemption has been discussed. The general effect of the first exemption scenario – explicit recognition of a legitimate secondary purpose – could be modelled alternately as a later stage in the *same* life cycle, a *new* life cycle, or a continuum *thread*.[37] The need with digital material to manage consciously the phases or dimensions of the record – whether consecutive or concurrent – ought to warn against injudicious fudging of this issue. Meanwhile, statutory regimes governing personal data in archives normally judge that "private," unpublished, "non-professional" research – such as genealogical research – does not constitute further disclosure of personal data.[38] This effectively cuts off the life cycle model at this point. It may even suggest that the research purpose is now the primary purpose of a *new* life cycle. On the other hand, "professional" research – particularly in bulk instance datasets and taking advantage of privileged access opportunities – in general requires the regulation afforded by a code of ethics until the material is available by open access. This can rarely be considered in isolation from the primary purpose: not seeing this as a part of the same life cycle makes little sense. In Canada, as records of the Government of Canada are transferred to Library and Archives Canada, the personal

36 Ultimately this can only be resolved by reference to the governance, participation, and accountability issues also raised by the records continuum.

37 The discussion on the previous page suggested that the "nesting" of a secondary archival purpose within the primary purpose is frequently how public archives regimes have operated in the past. This has dodged the issue by drawing a discreet veil over it, something few contemporary privacy regimes can allow. The viability of this as a single thread in a continuum viewpoint is fragile from a modelling, let alone a governance, point of view.

38 Case law on disclosed personal data about living extended family in on-line pedigrees, etc., would be an interesting if unwelcome problem for archivists to have to contend with. The main point is that this is an area that is at present exempt from further regulation, but that may change, especially if combined with concerns about genetic profiling, heredity, etc.

information they contain is deemed simultaneously to be "disclosed" to that institution. This hints to the present author towards a mixed economy of models: a single or a series of life cycles (in the latter case each relating to a single custodian), if not an all-encompassing continuum viewpoint.

The European data protection directive deals with role and responsibility issues by making almost everyone a "data controller."[39] It follows naturally enough that in the accustomed (life cycle) manner, the "private" researcher is normally exempt from this nomenclature and its responsibilities. Iacovino and Todd noted that whilst the jurisprudence behind the European Directive 95/46/EC might seem to imply the management of archives as a continuous process starting at creation, apart from the example of the Belgian domestic enactment of that Directive, the other legislative transpositions seem to be obstinately life cycle-based. The Directive itself requires personal data to be "processed" – a definition that includes, crucially, mere retention of records containing the personal information – only for a period concomitant with the purpose for which it was collected or a compatible purpose.[40] A "compatible purpose" under the Directive may include research, statistical, and historical purposes, but clearly needs to be identified if it is to sustain any challenge. The exemption for historical, statistical, and research purposes does not have to comply with the *fifth principle* that limits retention to a period linked to the primary purpose. From the archival perspective, this clearly requires identification as early as possible, irrespective of the agent retaining or processing the personal data (i.e., the creating organization *or* archives). Fortunately, continuum theory apart, this is in keeping with the recommendations of a number of authorities on digital records, from a variety of theoretical and methodological perspectives including the Appraisal Task Force of the first phase of the InterPARES project.[41]

There are areas, though, where application of more detailed consequences of continuum thinking may fall foul of the European jurisprudence.[42] The main challenge comes from the need to identify and isolate the "compatible purpose(s)" for which personal information contained within the archives will continue to be processed. As noted by Iacovino and Todd, different jurisdic-

39 Consequently, many of the challenges of the Directive to archival preservation discussed by Iacovino and Todd would be seen to bite on the activities of the records creator, at least viewed through the life cycle model. See also MacNeil, "Privacy, Liberty, and Democracy," pp. 80–81.

40 Destruction and – most significantly – undertaking preservation processes are also "processing" of personal data. There is probably some mitigation owing to the principle of proportionality, but it would be preferable for these essential archival activities to be defined as something else (but see footnote 35 above).

41 Duranti, ed., *Long Term Preservation*.

42 An alternative viewpoint would be to conclude that this merely demonstrates the translation that is required to convert such a model into a juridical instrument.

tions have articulated different permutations of research, statistical, scientific, and historical purposes. In general, they concluded[43] that there was no great practical significance in these differences. For the purposes of the present theoretical analysis, though, there are distinctions to be drawn: a number of specific exemptions allowed to archival processing rely on the identification of a formula equating to, or resembling "purely historical processing" of, the personal data.[44] This is challenging, the present author submits, not just for convinced continuum thinking. It strikes at the heart of what we consider as archival mission. We can perhaps understand on one level the motivation of legislators to eliminate normal administrative action from the options available to records creators, once the justification for the continued retention of the records is identified as "historical" and/or "research," but at the same time it seems to eliminate archival purposes that we as a profession ought to be active in promoting. The origins of the archives in the recognition of the societal value of the records and their place of residence as a place of power, rather than an association with redundant information of purely esoteric, academic, and/or solely genealogical value ought not to be forgotten. In addition, there may be more compellingly contemporary human and patrimonial rights issues to be supported by the archives.

There are other fundamental issues that also require a contribution from archival science if e-Government implementation is not to jeopardize documentary heritage. One is the emergence of types of data for identification or therapeutic use that is almost more sensitive than individuals' healthcare case information: their genetic profile. This could have a number of legitimate applications, but could simultaneously be seen as intrusive, oppressive, or open to abuse. It also challenges "sunset" provisions because subsequent generations may be as affected as the one about which the personal information was collected. The problem is brought into sharper relief by the multiplicity of agents commonly involved in implementing political programs, typically involving a mixture of sectors across public, private, and not-for-profit. The needs of regulating the flow of personal health data is one of the few privacy issues to have been recognized in recent American legislation, a measure necessary to balance the portability of health insurance between private providers. Other types of insurance, and suggestions that genetic profiling should be used as a measure of precise insurable risk, raise fundamental questions about both business models and privacy.[45]

43 See Iacovino and Todd.

44 The usual Canadian legislative formula is to exclude administrative action in respect of the individual based on the record(s) in question. Some regimes permit continued processing "for the benefit of" or insofar as it "is not detrimental to" the data subject, but give little help in determining whose viewpoint will be decisive.

45 More will be said about ambitious e-Government healthcare records programs later in this paper, when Livia Iacovino's work on Australia's Health*Connect* will be considered.

There are many other public/private e-Government issues close to significant digital archival issues. Only two examples can be discussed here. In a recent paper to a workshop run by the Public Administration Committee of the UK House of Commons, a group of academics called for the urgent input of information managers as well as technologists in policy discussions about e-Government. They saw the trend to be highly ambivalent as it relates to targeted service delivery rather than equal or need-based access. The rhetoric of empowering the citizen/consumer also introduces informational relationships not understood by, and opaque to, most citizens. The use of manipulative "customer relationship management" even amounts at times to covert surveillance:

> This context of ambiguity suggests that interpretations of the drive for citizen identification, whether undertaken for conventional e-Government services or for security reasons, may themselves be ambiguous ... enhanced access to service and product consumption made possible through new technologies carries a price measured by loss of privacy ... the highly "informated" individual can organise, travel to and deploy forms of terrorism outwith the purview of the individual nation state.[46]

Secondly, the use of commercial third parties as intermediaries to supply such enablers as digital signatures for e-Government transactions means that personal data has to be transmitted and entrusted to the private corporation just to enable participation in e-Government services.[47] If citizens are reliant on commercial providers for the establishment of their personal identity, what change is being implemented in the balance of power between Government, its intermediaries and the citizen?[48]

It might be argued that anything that limits the powers of an overweening state in handling personal information about its citizens, and gives them distinct rights over how that is done would seem to qualify for the epithet "postmodern." In fact, as with so many of the other methodological issues already mentioned and other postmodern deconstructions, the issue is one of many

46 J.A. Taylor, Miriam Lips, and Joe Organ, "Freedom with Information: Electronic Government, Information Intensity and Challenges to Citizenship," unpublished paper presented at the Public Administration Committee workshop on FOI, University of Durham, April 2005.

47 The InterPARES1 project investigated the problematic nature of digital signatures and further work has continued under the auspices of InterPARES2. See Jean-François Blanchette, "The Digital Signature Dilemma: to Preserve or Not to Preserve," presented at the Imaging Science and Technology Archiving Conference, San Antonio, April 2004. Some of the same civil law jurisdictions mentioned earlier as having enacted clear archival exemptions in response to the European Directive 95/46 EC may have created significant barriers for the archives with their enactment of the Directive 99/93 EC on eCommerce through the overenthusiastic substitution of asymetrical key digital signatures for manual ones.

48 It is noteworthy that the analysis in Livia Iacovino's articles on the Australian Health*Connect* system includes most of the elements of this political scientific analysis from a different methodological standpoint and with clearer archival science mappings (references below).

layers. Privacy is a concern of relatively advanced societies: it is very unlikely to be the first priority of those dispossessed of their patrimony. There is abundant professional literature about the role of the archives in acknowledging the identity of minorities, particularly those emerging from oppression or societal trauma. Drawing on philosophy from several centuries, Heather MacNeil[49] speaks of the integrity of the individual. It is true that a totalitarian regime is prone to invade the privacy of its citizens, but establishing the right to life and property require, at some level, the identification of individuals and knowledge of their rights and property. This is, at some level, information about personal affairs with well-established archival consequences.[50]

Jacques Derrida's *Archive Fever: A Freudian Impression* concerns itself with deconstruction of the archiving process, bound up with the psychoanalytic œuvre, personal life, and its archive – including the psychoanalysis – of Sigmund Freud.[51] For Derrida, whilst the archive is an instrument of power – even textual violence – to be deconstructed, he chooses to take his argument far beyond this most obvious of postmodern theses about privacy. For Derrida, this "violence" lies in the exclusion of alternative narrative constructs. Personal information, particularly that about the parties, plays a particularly significant role in the assertion of the construct experienced by the participants in both the action and the record creation process. Engaging with the full force of what is offered in this text, there are certainly wider but analogous issues with other forms of contextualization. This paper cannot attempt to deal with these comprehensively, but there are other compelling reasons to broaden the discussion of issues raised by *Archive Fever*. The postmodernist philosopher possesses a view of truth diametrically opposed to one we can accept as archival professionals.

Terry Cook reminded us that we have a number of modernisms that may or may not be "post," including twentieth-century Fascism, Communism, and perhaps even the claim that our profession possessed a definitive body of

49 MacNeil, *Without Consent*, is aware of the tension between "Documenting the lives of the labouring and unlettered," the title of her third chapter, pp. 103–127; and "Limiting the power of the state by the establishment of moral and legal zones of privacy," the title of her first, pp. 9–34.

50 Such as public land registers, including the one in Alsace-Moselle that is the subject of an InterPARES case study. Both MacNeil, *Without Consent*, and Terry Cook, "Fashionable Nonsense or Professional Rebirth: Postmodernism and the Practice of Archives," *Archivaria* 51 (Spring 2001), pp. 14–35, draw attention to the idea of the panopticon in the writings of Michael Foucault as an extreme example of state surveillance. Equally, it is worth remembering that identity theft associated with ethnic cleansing has occurred in contemporary conflicts in Africa and the Balkans. These are more basic examples of the contradictory aspect of privacy and rights than usually provoke comment, but see the reference to Ketelaar below.

51 Jacques Derrida, *Archive Fever: A Freudian Impression*, trans. Eric Prenowitz (Chicago, 1996), a notoriously difficult text, rendered far more comprehensible through the mediation of Brien Brothman in "Declining Derrida: Integrity, Tensegrity, and the Preservation of Archives from Deconstruction," *Archivaria* 48 (Fall 1999), pp. 64–88.

knowledge that can be called "scientific."[52] Heather MacNeil, in "Trusting Records in a Postmodern World,"[53] takes a broader sweep from the enlightenment philosopher, Locke and his *Essay on Human Understanding*. The present author would like to use a Victorian example about the related discipline of history, and then discuss some more aspects of the relationship between that discipline and our own. Thomas Carlyle famously declared in his *Essay on Heroes*: "the history of the world is but the biography of great men."[54]

Amongst our own profession, it does not take a convinced postmodernist to disagree with this statement, although in Carlyle's defence his main subject, a didactic need to promote heroic action and history, rather gets caught up in his rhetorical style. We could adopt more contemporary and inclusive definitions of what heroism and greatness are … and we had better not forget also to correct the sexist bias of the statement. So much is evidence of how far we have come from the origins of the archives as a power base of societal elites. It goes hand-in-hand with the broadening out of our understanding of history from the (elitist) political and legal to the social, socio-economic, and then into the establishment of a pluralism of histories including those of minorities, women, children, and so forth. The most mainstream postmodern challenge to our profession is essentially that: by theoretical constructs and practices related to the political function of the archive within the state, it introduces its own metanarrative(s), and cannot be an impartial purveyor of the past. Unfortunately, however this thesis is operationalized, further problems are created.[55] If the archives are to do more than act as the instruments of the power of political elites, they must provide the documentary basis for us to make sense of these alternative viewpoints. The author considers that an important part of this is to support the survival of narratives, rendering the relationship between postmodern agendas in historical and archival disciplines a symbiotic one.[56] This is a broader argument than that about *meta*narratives employed by Cook, Ketelaar, et al. The trouble is, the practice of records management and appraisal make greater interdisciplinary linkage inevitable.

Verne Harris has spoken of the presence of "whispers" in the archives, frag-

52 Cook, "Fashionable Nonsense."

53 Heather MacNeil, "Trusting Records in a Postmodern World," *Archivaria* 51 (Spring 2001), pp. 36–47.

54 First published in 1841.

55 Postmodern philosophy, with the luxury of not having to operationalize, would acknowledge its own existential problem. Archival practitioners have a more difficult time of it. This issue is returned to at the end of this paper.

56 Though some archival disciplines require distinctions to be drawn: see the discussion of the diplomatic tradition below.

mentary hints of broader experience even in the archives of past elites.[57] This has a long tradition: the distinguished medieval historian James Campbell made a great deal of dark hints in the Venerable Bede's *Ecclesiastical History of the English Church and Peoples* to enrich the possibilities of the state in seventh-century England, even where the hints betray some ambivalence on the part of the historian towards some of the heroes of the story. For example, there is the curt reference to the reason why the Monks of Bardney Abbey in Lincolnshire initially would not accept the remains of St. Oswald *en route* from his death at the Battle of Oswestry to his final resting place: "because he had come from another province and had ruled over them."[58]

We are close here to a profound differentiation between the historical and archival disciplines. The archivist's role is to preserve the documentary truth and, as such, can only act to preserve the traces of human action. Constructing a collective narrative from a series of fragments depends on there being enough to go on to support that narrative. Speaking very strictly, the archivist's activities of arrangement, editing, and description are constantly in danger of overstepping the blurry boundary into an historical interpretative discipline. This is a part of the argument about archival metanarrative articulated by Cook et al. from a postmodern viewpoint, but also the discussion in these pages about our interface with historians. Yet it remains true that historical revisionism has often been based on fragments of socio-economic data, so the power of archival "whispers" alone cannot be denied.[59] In a sense, though, they are not enough. To make sense of the experience of a broad range of histor*ies*, as a "trace" of humanity, there must be sufficient contextualization in the documentation. For this to convince and make present and immediate the

57 Readers of *Archivaria* will be familiar with "On Archival Odyssey(s)," *Archivaria* 51 (Spring 2001), pp. 2–13, but for the present author, Harris' presentation at a conference at the Liverpool University Centre for Archival Studies in July 2003 was particularly memorable. This presentation was published in Margaret Proctor, Michael Cook and Caroline Williams, eds., *Political Pressure and the Archival Record* (Chicago, 2006).

58 *Historica Ecclesiastica*, iii, p. 14. Bede wrote in the eight century drawing on – probably – a combination of documentary and oral sources. Most historical commentators have drawn this out as an indication of the nature of "overlordship" in seventh-century England: the (compatible) point here is Bede's narrative technique rather than the provenance of the latter in an archival sense. This and some of the other historical revisionist examples are chosen to show that it is not just social and economic historical sub-disciplines – often associated with postmodernism – that produce this phenomenon.

59 For example, evidence of social mobility and prices in early modern England fuelled the celebrated mid-twentieth-century controversy between R.H. Tawney and Hugh Trevor Roper over the former's claimed "Rise of the gentry" in sixteenth- and seventeenth-century England found in the *Economic History Review* 11 (1941) and its 1953 first supplement respectively. It is but one example of a deconstruction of a Marxist determinist thesis by such means, and an example of social historical debunking of elitist political narrative before "social history" existed as a distinct discipline.

experience of our predecessors, it must also include some personal information. Many of our users seek direct genealogical linkage to enable them to claim their documentary patrimony. In the absence of real personal information contained within the archives, archetyping seems the only alternative to sterile anonymity.

This brings us to the dilemma of considering privacy as a postmodern proposition. On the plainest level, reducing the ability of the state to interfere in the private lives of its citizens (even for benevolent motives[60]) is postmodern. Yet taking that to its logical conclusion would deprive the archive of their narratives, possibly fatally. To serve the other, second level, postmodern agenda of documenting plural histor*ies*, we need personal information about at least some of those people. Otherwise, we shall be restricted to fragmentary "whispers" about their stories. Alternatively, are we to take as the object of postmodernist deconstruction not just the narrative of the empowered, but *narrative itself*? This is heady stuff. Narrative seems to be a principal means of making sense of fragmentary sources for the human psyche, no doubt owing to our nurture. As practitioners we should not be denying our users the ability to make sense of the documents through the construction of narrative in *their* search for meaning. The issue is the awareness of our construction of meaning in our professional activities and the need to deconstruct that. To what extent, though, is this interpreting the documents, and how far simply preserving and making them available? At another level, though, narrative is very much a part of why we construct aggregations of documents: putting them together in a sequence so that the value of the whole is somehow greater than the sum of its parts.[61] A "sequence" is based on some principle, common attribute, or construct, and normally arranged according to a chronology.[62] In the digital environment, we are acutely aware of the existence of potential multiple views according to which particular attribute is seen as the most significant. Picking up on the issue of narrative in the previous paragraph: beside the explicit attribute of "subject," "transaction," or "case" (personal details?) there normally lurks an aggregation and arrangement principle based on the construct of chronology (our habitual historicism as a profession would normally prevent us from seeing this as anything other than an objective criterion:

60 Edward Higgs, a prominent British data archivist, offers an apology for the mass of information accumulated by the English state about its citizens on the grounds that its motives were benevolent and the state did not develop the machinery to use it consistently as a tool of oppression. See his *The Information State in England* (London, 2004).

61 Archival science differs essentially from the science of diplomatics in assigning primacy to the aggregation.

62 The question occurs to the present author, whether the adoption of a strictly functional principle to the aggregation of records might in some respects represent a deconstruction of concepts of "case" or narrative?

perhaps we inevitably have to see this as a deconstructive step too far?).[63] The primacy accorded to an aggregation principle in the creating environment is normally our touchstone as archivists, but we cannot protest innocence of involvement as a profession in the records management process. We maintain this through transfer of custody of records to the archives. For many records series, the attribute seen as "prime" will be some sort of personal identifier.[64] To the citizen who is the "subject" (or even the "object") of some e-Government transaction, this is the way they will perceive their involvement in the transaction also. Accountability for that transaction through its documentation is likely to be best served by it being used as the attribute that determines its fonds, its appraisal, and ultimately its disposition. Yet this is not different in principle from data matching: the difference is one of degree. It is acceptable, indeed necessary if the citizen's view is to match that of the bureaucratic processes and be comprehensible if they access official information about their "case." But if carried into an extent that is not expected or consented to, it becomes a violation of personal privacy.

At one point in *Archive Fever,* Derrida gets close to discussing the dilemma just arrived at:

> In the classical structure of their concept, a science, a philosophy, a theory, a theorem are or should be intrinsically independent of the singular archive of their history. We know well that these things (science, philosophy, theory, etc.) have a history, a rich and complex history that carries them and produces them in a thousand ways. We know well that in diverse and complicated ways, proper names and signatures count. But the structure of the theoretical, philosophical, scientific statement, and even when it concerns history, does not have, should not in principle have, an intrinsic and essential need for the archive, and for what binds the archive in all its forms to some proper name or to some body proper, to some (filial or national) filiation, to covenants, to

63 Many professional contemporary historians are not conspicuously interested in narrative – postmodernism in their professional milieu is at least partly responsible – but the point is a serious one. The sub-disciplines of social, economic, gender, and other histories have been successful in tempering the dominance of the history of the dominant political groups, in part by the promotion of a more "scientific" approach. This has also affected archival programs with the advent of data archiving. In this as in many nuances of the argument here, postmodernism(s) cut(s) both ways at this point too: whither the narrative aspects in the oral traditions of indigenous populations, personal genealogy, and local history?

64 It is interesting that many countries are wrestling with the privacy consequences of e-Government most urgently in the health sector. This is based in part on the consensus of the sensitivity of such information. On the Australian picture, see Moira Paterson and Livia Iacovino, "Health Privacy: The Draft Australian National Health Privacy Code and the Shared Longitudinal Electronic Health Record," *Health Information Management*, vol. 33, no. 1 (2004), pp. 5–11. It is also instructive that in the United States, the requirement for private sector health providers to share health data prompted the introduction of the *Health Insurance Portability and Accountability Act* in 1996 to regulate the privacy consequences. This article began by noting the general immaturity of privacy protection in the USA and the private sector.

secrets. It has no such need, in any case, in its relationship or in its claim to truth – in the classical sense of the term.[65]

Derrida was evidently of the opinion that the "truth" of information content must be allowed to float free and independent of the "violent" act of being fettered to a particular context. This must surely include the identity of particular participants and so much might be expected of a structuralist. This is an important point: as a profession we strive not to stray too far into the historians' task of interpretation, but the upshot of this argument is that in absolute terms this is impossible. So, we are to be allowed our "diverse and complicated ways" (archival science, anyone?) and it is even acknowledged that the binding of content identity "counts," but whilst for many of us it is an essential part of documentary truth and the establishment of authenticity, for Derrida it is immaterial to the "classical sense" of the content. It is clear that our mainstream professional notions of documentary truth are widely at variance with Derrida's on this point. It is interesting that in a number of significant respects, there are also echoes of our privacy management agenda. For example, Derrida assigns primacy firmly to the text, the *content*. If we recall the perceived duty to correct personal information that was accepted as accurate at the time of documentation: the integrity and hence authenticity of the record depends on the retention of the personal information as is and achieving a "correction" to the holding and future processing of the personal data should be achieved by annotation rather than expungement. "Classicism" in many disciplines implies a consensus on a stable, closed form. Even radical iconoclasm within a discipline could be – at least until the advent of something resembling postmodernism – essentially a stretching and manipulation of this form but depending very much on its still being recognized as being present, albeit under tension.[66] This use of the term "classical" to apply to content rather than to form is a peculiar one and one that shows many of us as being at the opposite polarity to Derrida on this point.[67]

It is high time to bring in the societal dimensions of the records continuum. The records continuum is, of course, about far more than an alternative model to challenge the life cycle viewpoint. Making explicit the "other" three dimensions of the continuum beyond the record entity itself, namely the business with its processes, mandates, and agents, requires consideration of the inter-

65 Derrida, *Archive Fever*, p. 45.

66 Examples might include Mannerist architecture and painting or any number of great works of music. The InterPARES2 domain working on reliability, integrity, and accuracy of digital records from dynamic, interactive, and experiential systems is conducting conceptual analyses of concepts of authenticity in the arts and mapping these to archival concepts.

67 This polarity is particularly marked with the diplomatic tradition, as one might expect. Terry Cook, in "Fashionable Nonsense," singles the latter out as representing an extreme "modernist" position. The reasons are readily apparent.

play between them. The conceptual arrangement of the entities thus wraps up the processes of archive building as integral parts of "other" processes. As a result, records creator and archival processes are expressed clearly as participants in the processes the records are subject to, rather than impartial gatekeepers. This has a number of consequences of direct impact on this discussion. The first is the inevitable alignment of the continuum viewpoint with postmodernism. The second is that our prime concern here, the examination of power issues applied to contemporary privacy, is greatly enriched by the literature of continuum exponents and adherents.[68] In theoretical terms, Eric Ketelaar's consideration of "Records and Societal Power" offers a number of challenging ideas about privacy. Concentrating mainly on dramatic case material where oppressive regimes have manipulated the identities of minorities, he offers some deep reflection on power and the personal information in archives.[69] This discussion is acutely aware of the dichotomy of the need to record the story of the dispossessed, yet also for the struggle against excessive state collection of information to continue. Then again, there is a need for the actions of oppressors to be recorded and their linkage to personal details of their victims for redress to be possible.

The requirement here is to draw out the general points of general application to archival thinking in circumstances less traumatic. Some of this has been done for us:

> Records in our surveillance society reveal as much about the administering as the administered. That is why it is so difficult to keep the balance right between, on the one hand, the requirement to destroy personal data when they have served their primary purpose, including that of serving the legal rights of the data subjects, and, on the other hand, the possibility that the files might get a new meaning and purpose in the future. Many of the files created during and after the Second World War, which are now being used in the processes of restitution of and compensation for holocaust assets, should have been destroyed. Such destruction was, not long ago, lobbied for by partisans of "the right to forget." Such destruction would have been in accordance with the criteria of data protection and privacy legislation and of most professionally accepted criteria for archival appraisal.[70]

68 A major collaborative book appeared during the preparation of this paper: Sue McKemmish, Michael Piggott, Barbara Reed, and Frank Upward, eds., *Archives: Record-keeping in Society* (Wagga Wagga, 2005).

69 Eric Ketelaar, "Records and Societal Power," in McKemmish et al., *Archives*, pp. 277–98. Many of the examples are drawn from or analogous to stories of restitution following traumatic societal events well rehearsed in the literature: what is most valuable is their presentation in this philosophical way.

70 Ibid, pp. 285–86. Ketelaar seems to be suggesting that the right to forget – or does he mean reconcile and perhaps forgive? – can only be served by the preservation of the archives of the trauma.

Ketelaar accepts that exceptional events require an exceptional response, including in appraisal as this quotation shows: what is less clear is whether he is calling for radical review of the "accepted criteria" for all circumstances. He goes on to consider the participation of the oppressed in the archive making of the oppressors in a way that a positivist "life cycler" would not. The overriding point behind the discussion of the record creation process is that it is not merely "what" the record records, but "how" it comes to do it that matters and this is plainly linked to identity:

> Those who were subjected to the power became subjects of the record created by that power. Formally, they had no voice in the creation and use of the record. However, by retrospective causality, they have to be considered actors in the semantic genealogy of the record and the archive too. Their power should be recognised as much as the power of creators and keepers.[71]

The attractions of this view of the power of the previously oppressed aside, such a view and especially the concepts of "semantic genealogy of the record" and "retrospective causality" are plainly incompatible with the InterPARES viewpoint as expressed in the *Authenticity Task Force Report*.

The old adage about "tough cases making for bad law" might be considered especially relevant at this juncture and for a number of topical reasons. One is the proliferation of a far more complex networked computing environment (Ketelaar calls ours a "surveillance society"). Another is the possibility that the response to the threat of terrorism may be a factor in shifting the balance in privacy protection: the response in terms of privacy may depend on whether this is an indefinite "war on terrorism" or a shorter engagement. In concentrating on the actions of several totalitarian regimes, perhaps the needs of a more plural society are not addressed directly, except insofar as Ketelaar considers the experience of Australia's indigenous populations. Certainly, the argument put forward by Edward Higgs begins to look a little weak given that a future regime's objectives may be different.[72] However, issues of consent are largely absent from Ketelaar's discussion: in a democratic society, whilst the level of participation varies, is it not the popular will embodied by the state contained in the will that caused the transaction and thus its record?[73] The collective *droit de mémoire* is effectively undermined by the exercise of the individual *droit de l'oubli*. The enshrining of the latter in the jurisprudence of data pro-

71 Ibid. Livia Iacovino has pointed out (in private correspondence) that the recipient of an action/data subject may be accorded certain use rights in the diplomatic viewpoint; see also Duranti, *New Uses*, pp. 85–86. Ketelaar takes this much further here, so far as to be sympathetic towards Derrida's viewpoints considered earlier.

72 Higgs, *Information State*.

73 This is not to deny the possibility of the oppression of minorities, merely to allow for a less monolithic view of "the state" (the author is aware that this is to make a positivist argument).

tection and privacy more widely seems to pose a significant threat to the archival mission and makes more urgent the recommendations that this paper started with. Heather MacNeil takes this a stage further: in a recent paper she raises the important point that in a less monolithic, more pluralist society, trust in the state's respect for individual privacy is undermined and the likelihood of consensus diminished.[74]

There is a trade-off between individual privacy and the collective memory. This is a too-little-discussed aspect of the social contract under which individuals cede liberty to public authorities in return for alternative benefits. In these circumstances, the argument runs, the contract that might exist between the right of collective memory is circumscribed by the level of buy-in to the giving up of individual privacy owing to a lack of consensus or stake in the collective consciousness. This argument has a postmodern dimension. If one of the tendencies of the rest of the argument presented here is a possible need for a new compact between public archives as trusted agents in the preservation and presentation of personal information, this then needs to be balanced by the complexity of negotiating a compact in a way acceptable to diverse interests. Derrida, though, seems to see the *droit de mémoire/l'oubli* dilemma differently. Memory, or rather its imprint, involves the exclusion of all other possibilities, the act of textual "violence." This turns the issue on its head: memory becomes essentially what we are unable – or perhaps not permitted – to forget. The text of Article 12 of the United Nations' *Universal Declaration of Human Rights* reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[75]

"Correspondence" is clearly meant to be interpreted widely for this Article to have much meaning. Just consider it narrowly for a moment: traditional literary biography has tended naturally to make extensive use of the formal recorded correspondence of prominent people and would be severely ham-

74 MacNeil, "Privacy, Liberty, and Democracy." This paper builds on an argument already present in the first chapter of MacNeil, *Without Consent*, "Defining moral and legal zones of privacy," pp. 9–34. It goes further, though, in considering circumstances of greater pluralism and in ways that may be important for the implementation of the recommendations of this paper: if the social contract between government and citizens is breaking down, how is consent to archival processing to be gained, except through archives stressing a role in governance and distancing themselves from government?

75 This dates from 1948. Consequently Article 8 of the 1950 *European Convention on Human Rights* reads: "Everyone has the right to respect for his private and family life, his home and his correspondence;" the second part of the Article continues: "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 prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

pered were this not to survive (Carlyle's "biographies of great men" [sic]). Yet if we are also to provide documentary evidence of lives "great" in other ways, including perhaps their ordinariness, and in our modern environment, we have more than one serious problem. The digital environment seems to suggest that we shall have to be far more intrusive and interventionist to collect their correspondence owing to its transitoriness and instability at the same time as the privacy agenda suggests that this is several steps too far. An extreme example of this was highlighted by the National Library of Wales representative at the 2003 UK Society of Archivists conference: the institution was proposing to capture e-mails of up and coming Welsh writers direct from their inboxes for later appraisal based on whether or not they became celebrated authors later.[76] Derrida was acutely aware of these fundamental changes brought about by electronic mail.

> But the example of email is privileged in my opinion for a more important and obvious reason: because electronic mail today, even more than the fax, is on the way to transforming the entire public and private space of humanity, and first of all the limit between the private, the secret (private or public), and the public or the phenomenal. It is not only a technique, in the ordinary and limited sense of the term: at an unprecedented rhythm, in quasi-instantaneous fashion, this instrumental possibility of production, or printing, of conservation, and of deconstruction of the archive must be accompanied by juridical and thus political transformations. These affect nothing less than property rights, publishing and reproduction rights.[77]

Much prosaic records management guidance about the management of electronic mail even acknowledges the "personal" space of the electronic mailbox and the level of intrusion required to gain corporate control over its content. Drawing a line between the extreme positions here will always involve an element of arbitrariness and will be a fine balancing act. In the European Union, all other things being equal, employers arguably have an obligation arising from Article 8 of the *European Convention on Human Rights* not to deploy server-side solutions to e-mail management. The issue is that even with appropriate use statements to the contrary, the receipt of a personal e-mail by an employee would render its manipulation a violation of their

76 A paper by Sara Hodson on the privacy implications of archives of authors and celebrities, albeit mainly concerned with traditional formats, has recently appeared. See "In Secret Kept, in Silence Sealed: Privacy in the Papers of Authors and Celebrities," *American Archivist,* vol. 67, no. 2 (Fall/Winter 2004), pp. 194–211. The present paper has only been able to make scattered references to the position of private archives. Mapping the implications for private archives of both the digital environment and enhanced privacy protection would be a worthwhile topic of further research beyond the valuable papers in *Archivaria* 52 and Tim Cook's article in *Archivaria* 53.

77 Derrida, pp. 17–18.

privacy. Instead, either individuals have to give explicit consent to the monitoring and capture of their correspondence or they have to be given direct and ongoing control of what enters the "corporate" domain.

This paper proposes that distinguishing between the several layers of postmodern analysis and rights of the individual is essential if the privacy agenda is to be discussed productively in such a context. Broadening out the canvas now to other theoretical viewpoints permits renewed consideration of issues of power, consent, and the archival implications. The likely precedence of concern about patrimonial rights, personal identity, and views of the purpose of "historical" archives over privacy has already been touched upon. At a lower level, the threat to the integrity of the record from the obligation to correct inaccurate personal information they may contain must be viewed in its wider context. Accordingly, Iacovino and Todd recommended that this be best implemented by annotation rather than expungement, for human rights as well as archival integrity reasons:

> Liability arising from incomplete or incorrect information may give rise to damage claims by parties affected. Therefore to prove that incorrect information was provided there needs to be evidence of what was seen by the parties. The deletion of inaccurate personal data can in fact lead to the absence of evidence of the incorrect personal data used in further action.[78]

In addition, this issue takes us considerably beyond public law of privacy and data protection, not to mention FOI. We get instead into the (private) law of confidentiality. It will be a commonplace point to readers of *Archivaria* that the participants in the records creation process have distinct viewpoints, although we may be able to reconcile their interests and moral obligations at a theoretical and methodological level.[79] Records of the various parties might contain much the same content quite differently arranged and identified according to whether it was created or received by them.

MacNeil follows through in ample measure on her declared intent to examine "The ethics of *disclosing* personal information in public archives."[80] At the same time, her discussion of the balancing of FOI with privacy concerns in the United States and Canada does consider this point from the records creation and maintenance perspective when she discusses the increased scrutiny afforded in Canada where the activities of an independent privacy commissioner throw light on some records management practices. This paper has

78 Iacovino and Todd. These authors reference Daniele Laberge's very immediate example, "Information, Knowledge and Rights: the Preservation of Archives as a Political and Social Issue," *Archivaria* 25 (Winter 1987–88), pp. 44–50.

79 Livia Iacovino's more detailed consideration of the moral rights and obligations dimension is discussed below.

80 Present author's emphasis: this is in fact her subtitle to the main title, *Without Consent*.

already outlined the need at this point to encompass also the fundamental issues of having consent to appraise and hold records containing the personal information in the first place. "Consent" must imply either an involvement in the records management (usually records creation) process or some subsequent access right.[81] A very broad "participation/consent matrix" might be constructed along these lines to articulate some of the issues in the creation of records:

	Agent	**Subject**
"Active"	Creator	Prime
"Passive"	Recipient of action (/Addressee)	Incidental

The main point to draw out is that the four different scenarios articulated here give privacy and consent issues of different orders of magnitude and management. Along the "active" axis, the agents are most empowered, although if privacy exemptions overriding data subject access were/are in force, the subject may, exceptionally, not be aware. With respect to "passive" access, neither the recipient nor the incidental data subject may be in a position to give explicit or implicit consent[82] (the participants' perspectives, understanding, consent, and moral rights/obligations might be quite different). Further, whilst much of the discussion hitherto in this paper has concentrated on the archival issues implied by personal information about participants in the process of creating the record, the most disempowered party is the subject of the incidental reference with no part in this process, even more so if (s)he had no role in the business act that gave rise to it.

The most dramatic example of these different perspectives involves bringing the argument further back into the issue of access management; specifically, public FOI policies. Many FOI regimes explicitly avoid disrupting the (normally *private)* law of confidentiality, although the two-centuries-old Swedish law demands the release of information about a public authority's business notwithstanding the presence of personal information, incidental or otherwise. Such an approach risks a public authority being unable to some degree to account for its actions.[83] This may not be particularly contentious if

81 In practice this is subsumed in the consent implied by the social contract the citizen has with the state.

82 Though they emphatically **will** be in the specific scenario highlighted by Livia Iacovino. The wider point here is whether the general trust in public authorities and public archival institutions will bear archival processing as acceptable.

83 The usual formula for accountability to the wider public is for the case records to be kept private while the case handling *system* is based on *disclosable* standardized workflows. Additional assurance is provided by independent auditors with trusted and privileged access to a sample of the data.

there is no wide interest in a particular case. There will inevitably be cases where there are difficult clashes emanating from this cause and arguments about whether any public interest override in the access regime is brought into play. Other regimes seem to impose a duty on public authorities, including archives, to employ extensive and expensive redaction to reconcile the differing requirements. This could serve further to undermine perceptions of the integrity of archives[84] noted in the introductory sections of this paper. Privacy and FOI regimes vary in their apparent respect for the integrity of the record. Those that only deal with the disclosure aspects – typically by creating a right of FOIA access to information rather than to the records – tend to neglect this.

This alternate public and private view requires some further development at this point as it relates to those in public life. Was the dual nature of prominent lives – partly public and partly private – understood actually as a justification for our having documented their narratives and processed their personal information? This is a very live issue on both sides of the Atlantic, as witnessed by case law where celebrities have attempted to reduce press intrusion.[85] And what are the consequences of this thought for the documenting of more "ordinary," "private" lives that would otherwise be accorded the dignity of obscurity?[86] This point reconnects us with another very old positivist archival concept: the public and private nature of documents.[87] Here again, the diplomatic tradition has something very precise and instructive to offer us, even striking to the heart of the difficult problem of separating the public and private domains.[88] Luciana Duranti's third essay on diplomatics[89] expounds this in detail. She does this in two main ways: first by distinguishing the historical from the documentary truth in a way entirely compatible

84 Constraints of space and scope preclude extensive consideration of whether historical analysis is served or hampered by the limited release of archival material. It is worth noting that Derrida was interested in this issue (*Archive Fever*, pp. 55–56).

85 The case brought by Michael Douglas and his wife Catherine Zeta-Jones against *Hello!* magazine for publishing unwelcome photographs of their wedding, although they had sold the publicity rights to an competing publication, is perhaps the most bizarre example.

86 Broadening of participation in public life, as this paper goes on to consider, can only lead to a corresponding increase in the proportion of what is deemed to be public.

87 A fellow researcher in the Policy group of the InterPARES2 project has offered a taxonomy for delineating the two domains in the United States based on historical usage and content analysis. See Terrence Maxwell, "Parsing the Public Domain," *Journal of the American Society for Information Science and Technology*, vol. 56, no. 11 (2005), pp. 1130–39.

88 No apology is about to be offered here for bringing together once more the issue of public vs. private fonds and the issues of access management. In addition, the empowerment of the citizen as either data subject, business process participant, or through freedom of information policies will tend to **increase** the public exposure of public fonds, something noted by MacNeil, *Without Consent*, pp. 50–54.

89 Duranti, *New Uses*.

with our discussion of an inaccurate record containing erroneous information but nonetheless accepted at the time of transaction/record creation; and secondly, by distinguishing between the public (or private) *will* that can be inherent in *both* parties' sides of the correspondence.[90] Further, where public policy agendas (e.g., FOIA) dictate enhanced public access to official records, the boundaries of what is *pertinent* require to be firmed up as a consequence. We can see, quite readily, that much sensitive personal information may not be of wide pertinence. We might in the past have been in a position to retain it until it was no longer sensitive and hence take it into archival custody, but that may now be in question.

Livia Iacovino's work on the moral rights of record-keeping participants presents both a more practical slant on the application of continuum and postmodern archival theory, and a valuable study of how moral obligations and societal ethical behaviour as well as formal juridical instruments shape records management practice. Taking the question of juridical governance, and moral and ethical behaviour first, Iacovino considers juridical governance from a broad perspective, including not just formal juridical instruments, but also moral rights and obligations that may not be explicit in the law but are nonetheless present in the environment within which records are created and maintained.[91] This approach is helpful, *inter alia*, in that it stresses both broader societal relationships and ethical behaviour along with the underlying jurisprudence that informs the law. Notwithstanding that privacy is a right that happens to have been enacted in most jurisdictions, this is particularly helpful in understanding the deeper forces in play.[92] If "the positivist tradition of jurisprudence limits law to rules backed by coercive sanctions in which power and state are co-dependent,"[93] most of us would agree that there is a line beyond which the state would be impinging on the private life of individuals, and this line requires legal definition and sanction. She touches on issues already discussed in this paper within this context: "The 'privatizing' of public law is an important change that alters a long-standing relationship between citizen and government and the role of record-keeping in that relationship."[94]

90 This has important echoes of the points raised earlier about e-Government implementation and their inherent power relationships.

91 Livia Iacovino, "Recordkeeping and Juridical Governance," in McKemmish et al., *Archives*, pp. 255–76.

92 After all, a record-keeping system can hardly support the protection of privacy rights without the concomitant policy framework.

93 Iacovino, "Recordkeeping and Juridical Governance," p. 255.

94 A staggering coda to this point and the contracting out of e-Government delivery is the awarding of the contract for the next Canadian federal census to Lockheed Martin, a United States corporation subject to the disclosure provisions of the US *Patriot Act*. Sample press coverage accessed at <www.theglobeandmail.com/servlet/story/RTGAM.20041009.wcens1009/BNStory/National> (accessed 13 March 2006).

Still more pertinent, there is a working through of the continuum model into a matrix of record-keeping processes and then the elements relating to individual identity:

> The degree of reliability of the contents of a record depends on how much is captured of the identity of the persons involved in the record's creation, their credibility, their authority (their competencies) and the consent of the parties to the transaction. Validation or certification of the parties to a transaction, or of the authors and recipients, depends on controls in the record creation process ... The assignment of legal responsibilities to "persons" is an indication of their property rights in records, or of their rights to the data or intellectual content in records, or of what they can do with the information. If we add third parties, which have an interest in legal relationships, we can come up with a useful matrix to identify recordkeeping participants in any legal system. In ethics, all the categories would also be moral agents ...[95]

On the Australian health sector,[96] Iacovino offers a robust archival and juridical critique of the logical design of the proposed "Health*Connect*" system. This has common aims with many similar programs in other countries: of engineering a "longitudinal" healthcare patient record system at the local service provider, state, and Commonwealth levels in Australia. This is a large, complex e-Government program – and one involving a multiplicity of partners, complex system architecture, and records management challenges including the public/private partnership trust issues aired earlier. As different views of the system design are considered, the identification of the record and its aggregation from discrete data shifts in a way entirely consistent with the definition of a record offered in ISO 15489.[97] Mapping such a pragmatic definition[98] to the more rigorous demands of archival methodologies, including continuum theory itself, is a more complex proposition, but this is also offered by Iacovino.

There are three main points to bring out from this work.[99] The first is that in a complex, distributed network environment, the safeguarding of privacy is a

95 Iacovino, "Recordkeeping and Juridical Governance," p. 267. This raises broader generic concerns than privacy, but some of them interface in indirect ways with protection of personal information: such as whether a private record depositor might wish to withdraw records held in the archives.

96 Livia Iacovino, "Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and Health*Connect*," [Australian] *Journal of Law and Medicine*, vol. 12 (2004), pp. 40–59.

97 Available at <http://www.iso.ch>.

98 The origins of ISO 15489 in AS 4390 must involve some caution not to infer a distinct continuum viewpoint in some of the wording: the definition of a record offered in ISO 15489 in terms of the business activity that produced it shows its continuum basis, despite the standardization process. The subsequent characteristics of a record show the trace of other archival traditions.

99 Other significant digital archival issues are also present, such as the problematic nature of the proposal to use public key infrastructure (PKI) to authenticate the integrity of digital objects and provide security through cryptographic techniques.

difficult business. This is the more so owing to the presence of sensitive personal data – albeit unlikely to be appraised as of archival value. The discussion offered has far more general application to e-Government solutions generally. The danger of personal information being transmitted to other parties and used for purposes unknown and perhaps unacceptable to the data subject is particularly acute. The second point is that the stated policy objective of giving the patient the right to correct or withdraw personal data from the system that had the potential to make the data subject an active participant in the record-keeping process had not been followed through in the design proposals available for analysis at the time of the study. Lastly, and most pertinently for this analysis, Iacovino proposes the view that the records management requirements, apparent in the outline of the system, are inadequate for the satisfaction of basic archival requirements including those of the InterPARES Authenticity Task Force.[100]

The notion of the records' form, content, and even their identification undergoing mutation in this way is one to conjure with and Livia Iacovino does not miss the contradiction between the logical consequences of the claims made on behalf of Health*Connect*, and the inadequacies of the articulation of a records lifecycle paradigm included in the implementation proposals. Rather than seeing this mutation as a change to any established fixity of the record, it is articulated as a prolongation of the creation process to a perpetual state. This notion of records being constantly "in a state of becoming," is an argument that has been expounded by Upward, McKemmish, and others[101] and is central to continuum thinking. Iacovino is explicit that this represents a change to the provenance of the record(s):

> the reliability of the contents of a record depends on how much is captured of the identity of the persons involved in the record's creation, their credibility, authority and competencies, and the consent of the parties to the transaction, while authenticity depends on ensuring that the record's integrity (completeness) has not been compromised[102] ... effectively, the right to enter and amend data makes the patient a record creator with responsibility for ensuring his or her own record is accurate and reliable, and may have legal consequences. If the patient has rights over what is documented, and how it is used (consent rights over specific kinds of information), he/she is a dynamic agent rather than a passive subject of the record; therefore, in addition to the changes in the record's provenance, the patient's rights and obligations are extended in the shared electronic health record model.[103]

100 Duranti, ed., *Long Term Preservation*.

101 Sue McKemmish, "Are Records Ever Actual?," in Sue McKemmish and Michael Piggott, eds., *The Records Continuum: Ian Maclean and Australian Archives' First Fifty Years* (Clayton, 1994), pp. 187–203.

102 Iacovino, "Trustworthy Shared Electronic Health Records," p. 49.

103 Ibid., p. 46.

This is very close to what Eric Ketelaar calls the "semantic genealogy" and "retrospective causality" of the record and strongly contrasted with the InterPARES1 viewpoint.[104] It is also interesting that without obligations to match the moral rights of the patient, there may be a serious problem with the reliability of the record:

> ... the admission that the Health*Connect* record will not be accurate and complete because individual events may not be reported, and the system is voluntary, immediately threatens its reliability as evidence[105] ... in the business processes that deal with receiving and storing event summaries, there is neither an explicit acceptance of responsibility of the content of the record nor the capacity to check contents between the source system and Health*Connect*.[106]

At the time of writing, with the serious challenges noted at the beginning to the preservation of identifiable personal information, it is salutary to note the pertinence of the different postmodern layers offered here. It is also interesting to note that for the most part these layers have little coherence and indeed are contradictory: this is one of the characteristics of postmodernism and it is the obverse side of the critique that it "tears down" and cannot "build up."[107] Privacy also offers very serious challenges to several other, perhaps even most, theoretical traditions and methodologies. The outcome of the discussion is patently inconclusive, except that we might use it as a counterweight to other ways of thinking and to subject our professional practices to healthy and rigorous challenge.

Perhaps this questioning is the most valuable contribution to our profession offered by postmodernism, something that can be appreciated even by archivists of a positivist stance. Similarly, Heather MacNeil and Livia Iacovino have proposed differently articulated privacy strategies that seem to the present author to have a lot in common with each other and significant concordance with a plausible postmodern viewpoint based on participation and therefore on consent. The distinction is that MacNeil's nexus of participation lies in the democratic process, Iacovino's in the interface between the record-keeping process and the moral and juridical frameworks surrounding it.[108] One is tempted to

104 Ketelaar, "Recordkeeping and Societal Power," p. 295.

105 Iacovino, "Trustworthy Shared Electronic Health Records," p. 51.

106 Iacovino, "Recordkeeping and Juridical Governance," pp. 255–76.

107 Cited in Cook, "Fashionable Nonsense," p. 14.

108 This is articulated from a records continuum point of view, though this is consistent with Heather MacNeil's statement "the main premise of [data protection] laws is that the personal information individuals must disclose to the government in connection with any of their transactions with it should be held to a trust relationship and should create a duty of non-disclosure, subject to specific and limited exceptions. When government records containing personal information are transferred to archival custody, the responsibility for preserving that trust passes to the archivist." See MacNeil, "Privacy, Liberty, and Democracy."

speculate, though, whether the philosophical stance of these analyses is in fact complexity rather than postmodernism. MacNeil's discussion centres on whether the limitations of the "seclusion model" should prompt its substitution by the participative, "informational self-determinative" model:

> The problem with the information seclusion model is that it tends to situate the essence of privacy in the ability to choose it and see that the choice is respected. The power of choice is emphasised rather than the way in which such power should be exercised. The privacy as participation model, on the other hand, is more concerned with sorting out the conditions under which personal information may be shared or withheld, based on an assessment of the consequences of that sharing or withholding for both the individual and society.[109]

This paper has found that there is some common ground between the outcomes of different theoretical and methodological approaches to the privacy "problem." The author submits that the debate is well worth having, a sign of a vigorous profession. Even polarized conceptual viewpoints can probably agree on most of the practical steps now needed. Colleagues such as Iacovino and MacNeil both seem to require the building of a new consensus based on trust in both the records creators' and archival processing of personal information. This will of course affect not only the issues discussed in this paper, but also the ethics of disclosure of personal information elaborated in our professional literature. It will need to be led with an awareness of the wider rather than the narrower view of both privacy and postmodern agendas as they apply to the practice of archives and archivists. This imperative seems to suggest that an additional policy recommendation needs to be promoted to the front rank of those already arising from previous research: namely the need to articulate explicitly the broader public interest served by the archival mission in rapidly changing technological circumstances, something also called for by Heather MacNeil.[110]

Promoting such a policy objective is not going to be straightforward in the current climate for reasons noted earlier in this paper, but this raises rather than diminishes its importance. It will require a far more informed discussion than appears to be conducted currently in many jurisdictions surrounding the management of personal information, as the examples mentioned earlier will illustrate. We as a (public service) profession perhaps owe many of our current privacy exemptions to our position in the machinery of government. This will suffer from a decline in trust in state information management in the current climate. If we distance ourselves decisively from this positioning, we shall have to find another way of getting the urgency of the privacy "problem" recognized by legislators. This may well have begun with the witnesses to the PIPEDA debates, but must be continued.

109 Ibid., pp. 75–76.
110 Ibid., pp. 80–81.