No.6

EAST ASIAN ARCHIVES

PROCEEDINGS OF THE FOURTH GENERAL CONFERENCE OF EASTICA ON ÒRECORDS APPRAISAL AND PRESERVATION OF ELECTRONIC RECORDSÓ

(8th-12th November 1999 Hong Kong)

PUBLISHED BY EASTICA
September 2000

The Long Term Preservation of the Authenticity of Electronic Records

by Professor Luciana DURANTI

School of Library, Archival and Information Studies

University of British Columbia

The records generated by society in the course of its activities need to be preserved, sometimes permanently, as critical instruments of accountability, as means of protecting individual, corporate and government rights, and as sources of information, research and study. Physical care of records is not sufficient, however, to ensure their preservation for the protection, perpetuation, and advancement of modern society. The authenticity, retrievability and accessibility of the records that are to be kept in perpetuity must also be guaranteed. This endeavour traditionally has fallen within the mandate of the archival profession, which has carried out its responsibility by storing, describing, and making records accessible to researchers for centuries after their creation. New information and communication technologies, however, have transformed the very meaning of the term preservation.

The last decade has generated more recorded information than any previous decade of human activity. The fact that the majority of these data is less accessible than ever before is one of the ironies of the modern information age. Idiosyncratic software systems generate, manage, and store digital information using technologies and media subject to the dynamism of the computer industry. This digital information gets lost in a self-perpetuating and expensive cycle of obsolescence and incompatibility. As a result of media fragility and technological obsolescence, the term preservation as applied to electronic records no longer refers to the protection of the medium of the records, but to that of their meaning and trustworthiness as records.

More importantly, organizations and individuals generate records in a variety of media and formats. It is quite common for records relevant to a single matter to exist partly in a paper file, partly in an email box, and partly in a spreadsheet application or in a relational database. It is difficult enough to establish and maintain the essential links among these records while they are being actively used. At this time, it is not known how to preserve such links over the long term so that, one hundred years from now, users will be able to see the entire dossier relating to the matter they are exploring, thereby understanding each record in context as well as the development of the affair.

Ad hoc attempts have been made to reduce all records produced by an office to a single medium, for example, by printing out email and inserting it in a paper file, by scanning paper documents into electronic systems, or by converting electronic and paper records to microfilm. These attempts have been unsuccessful for a number of reasons. First, the conversion of records only for preservation reasons hampers the flow of work in the office, and therefore its implementation tends to be sporadic and inconsistent. Second,

many records do not lend themselves to such conversion. For example, hypertext records cannot be printed out to paper, and scanned maps or photographs are not always reliable substitutes for the paper originals. Third, court decisions have rejected the practice of converting electronic records to other media on the grounds that the converted records lack elements critical to their use as evidence.[1] For example, the printout of an electronic spreadsheet will not contain the formulae on which calculations are based.

The effects of the adoption of information and communication technologies without forecasting and planning for the consequences of a hybrid records environment, media and digital obsolescence, and the proprietary and idiosyncratic nature of applications, have already been witnessed in government and other organizations. For example, at the German Federal Archives headquarters in Koblenz, archivists are attempting to save thousands of computer files and databases from the former East Germany. They contain the records of the ousted communist administration, including agricultural files and labour statistics, penal registration lists, and personnel files of party functionaries. However, the documentation of the digital systems on which the records were generated is missing, the software codes are unknown, and the storage media themselves are obsolete and in poor condition. Consequently, the electronic records of East Germany are lost to the new German government that needs the information they contain for administrative purposes, to the citizens whose interests are implicated in those records, and to present and future researchers the world over.

Lack of authenticity presents a problem as serious as lack of accessibility. Authentic records are records that can be proved to be what they purport to be, immune from any sort of tampering and corruption, that is, records that are trustworthy as records. RecordsÕ authenticity depends on their mode, form and state of transmission as drafts, originals or copies, and on the manner of their maintenance, preservation and custody. An example of the problems presented by the inability to prove that records are authentic is offered by the Somalia Affair. During the spring of 1996, the inadequacy of procedural mechanisms for ensuring the authenticity of electronic records became a focal point of hearings held by the Canadian Commission of Inquiry into the Deployment of Canadian Forces to Somalia. As part of its investigation, the Commission requested access to National Defence Operations Centre (NDOC) logs, which were maintained in an automated database and which contained a record of all message traffic coming into National Defence headquarters from Canadian ForcesÕtheatres of operation. During its review of the logs, the Commission discovered several anomalies, including entries containing no information, missing serial numbers, or entries with duplicate serial numbers. The Commission was concerned that there may have been deliberate tampering with these logs. Although subsequent investigations were unable to show evidence of tampering, they could not exclude the possibility of it, because of the absence of standard operating procedures with regard to the log, the complete ineffectiveness of the security system in place, a lack of system audits, and the tendency of officers to bypass the awkward system. Therefore, the Commissioners concluded that NDOC logs were not a reliable record of transactions at the operations centre either for present investigators or future researchers.[2]

The Canadian case shows that there will not be much worth preserving for the future if serious measures are not taken by records creators to guarantee the trustworthiness of electronic records since the moment of creation (in both meanings of trustworthiness of content and trustworthiness of the record as a record). Several of these measures have been identified by a research project on the integrity of current and semi-current records, conducted by the University of British Columbia, in cooperation with the Department of Defense of the United States, in 1994-97.[3] This research has produced, among other things, the records management standard 5015-2 for the federal government of the United States.

The first such measure consists of embedding procedural rules of records creation in an agency-wide, centralized records system, and of integrating business and documentary procedures. The second measure consists of instituting procedures for strengthening the recordsÕ interrelationships and the links that they have with the non-electronic records created by the same organization through an integrated classification system, registration, and the creation of a record profile for each record of the organization, electronic and non-electronic. The third and final measure is the integration of the management of the electronic and non-electronic records belonging in a hybrid records system.

In addition to these general overarching methodologies for ensuring that all records in a hybrid record system are created trustworthy, more specific requirements were identified by the same research project for the control of the electronic records within the system, such as:

¥compiling records according to pre-defined standard formats and templates;

¥authenticating records using pre-established methods, depending on record type and function;

¥embedding in the electronic records system access privileges, by assigning to each person who has access to the electronic system, on the basis of clearly identified competencies, the authority to compile, classify, annotate, read, retrieve, transfer, or destroy only specific groups of records;

¥embedding in the electronic records system Òworkflow rulesÓ according to which the system will present only the person competent for each action with the related records and will solicit the making of the appropriate record at the proper time in the automatic development of the procedure;

¥limiting access to the technology or to parts of it by means of magnetic cards, passwords, finger prints, etc.; or

¥designing within the electronic system an audit trail, so that any access to the system and its consequences (e.g., a modification to the record, a deletion, an addition) can be documented as they occur.[4]

Although the implementation of these requirements also supports the ability of the organization and of its legitimate successor(s) to verify or prove the authenticity of its electronic records, it is not sufficient to fulfill this purpose. Audit trails, encryption and the unique identification of the original version of a records may prevent, impede or detect manipulation and tampering while the records stay in the live system in which they were made or received and set aside. However, these means are not useful when the records are removed from the system either to be stored on a non-online medium or to be transferred to a new digital system.

A key difference between electronic and non-electronic records is that the latter are kept authentic by maintaining them in the same form and state of transmission in which they were made or received and set aside, while the former are kept authentic by continuous refreshing and periodic migration.

However, while refreshing generates a complete reproduction of both the content and the formal elements of the records, migration, which is the transfer of the records from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation, creates a reproduction of the content of the record, with changes in configuration and format, often having a ripple effect on other components of the record. Thus, the records resulting from refreshing may be considered faithful copies of the original records, while those resulting from migration always sustain some measure of loss.

There are components of the record that can be lost without compromising its substance and the ability to verify its authenticity overtime, and others the loss of which would be equivalent to the loss of the record. These components vary from a type of record to another. For example, color is a meaningful part of the message in a map or a chart, columns in a table, highlight in a hypertext, etc. In some types of records, these components are visible to the user, because they appear in their intellectual form. In others, they are invisible to the user, as they exist either as metadata or as the elements of physical form that condition, for example, the recordsÕperformance, that is, its sound or the speed at which the images in it move. Thus, it appears to be essential,

¥first, to identify for each type of electronic record produced by an organization the components that ensure its authenticity over time;

¥second, to assess whether those components that are not visible to the user can be made visible and stabilized by linking them inextricably to the intellectual form of the record;

¥third, to determine whether, in the cases in which this operation were not doable, it would be possible and advisable to move the records in question to a non-digital form (e.g., microfilm); and

¥fourth, to adopt self-authenticating and well-documented procedures for migration and an uninterrupted line of physical custody.

On the basis of pure common sense, the latter seems to be the most secure method to allow the verification of authenticity over the long term. When the records are needed by the creator in the usual and ordinary course of business, the procedural controls on records creation and maintenance established to ensure their trustworthiness, and the continuing reliance of the creator on the products of the refreshing and migration processes are by themselves sufficient to authenticate them. However, when the records are no longer needed by the records creator to conduct its business, but must be retained for any of a variety of reasons, the migration process will have to be carried out by a party who has no stake in the records content or existence. Moreover, its results will have to be verified and certified by such neutral party, be it an archival institution, a notary or any other body formally entrusted with an authenticating function. Finally, the resulting authentic copies of the obsolescent records will have to be declared so on the basis of a proper documentation of the process. Historically, archival description has always had the function of authenticating the records by making explicit and perpetuating their provenance and interrelationships. Today, its role is enhanced by the need for an ongoing description of the transformations to which electronic records need to be subjected time after time after time. It appears that, over the very long term, the only reliable form of authentication that will remain valid across cultures and regimes is one completely external to the records it validates.

However, this conclusion, as said earlier, is only based on common sense and needs to be demonstrated by systematic analytical research, recognizing that authenticity over time needs to be based on requirements and procedures independent of specific contexts and technologies, given the fact that future contexts cannot be known or predicted. Therefore, an interdisciplinary and international team of researchers has joined forces to address preservation issues in a theoretical way. The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) aims to formulate principles and criteria for the development of international, national and organizational policies, strategies, and standards for the long-term preservation of authentic electronic records. It is directed by myself and carried out by national and multinational research teams from various countries, including, among others, Canada, the United States, United Kingdom, Ireland, Sweden, The Netherlands, Italy, Australia, Hong Kong, and China. A global industry team includes multinational companies in the pharmaceutical, biochemical, health and computer fields.[5]

The research project is based on the concepts developed in the course of the previous research project directed by the University of British Columbia. In addition to the concepts of reliability and authenticity, it uses the decontextualised definition of record that identifies and defines its necessary and sufficient components, so that they can be recognised and captured by a digital information system. According to such definition, the necessary and sufficient components of an electronic record are the same as those of its traditional counterpart, although they may manifest themselves in different ways. They are:

¥medium, that is, the physical carrier of the message;

¥content, that is, the message that the record is intended to convey;

¥physical and intellectual form, that is, the rules of representation that allow for the communication of the message;

¥action, that is, the exercise of will that gives origin to the record;

¥persons, that is, the entities acting by means of the record;

¥archival bond, that is, the relationship linking each record to the previous and subsequent one; and

¥context, that is, the juridical, administrative, procedural and documentary framework in which the record is created.

The InterPARES research project is divided in four domains. The first domain aims to identify the requirements for preserving authentic electronic records. The research questions being addressed are directed at constructing a typology of electronic records based on their form, identifying for each type of record what are the elements that allow for the verification of its authenticity in time and over time, and developing a series of requirements for maintaining the authenticity of electronic records for as long as they need to exist. The research questions are:

1. What are the elements that all electronic records share?

2. What are the elements that allow us to differentiate between different types of electronic records?

3. Which of those elements will permit us to verify their authenticity over time?

4. Are these elements for verifying authenticity over time the same as those that permit us to verify their authenticity in time (i.e. at the point at which they are originally used)?

5. Can those elements be removed from where they are currently found to a place where they can more easily be preserved and still maintain the same validity?

The second domain aims to establish whether, in order to satisfy the requirements for authenticity identified in domain one, the appraisal criteria and methods for electronic records need to be revised or even radically changed. The research questions are:

1. What is the influence of digital technology on appraisal criteria?

2. In what ways does appraisal differ depending on the type of system prevalent in each phase of computing?

3. How do the medium and the extrinsic elements of the records influence appraisal?

4. How do retrievability, intelligibility, functionality, and research needs influence appraisal?

5. Should restraints be imposed on the modification of systems at the time of appraisal?

6. Does the life cycle of electronic records differ from that for traditional records?

7. When in the course of their existence should electronic records be appraised?

8. Should electronic records be appraised more than once in the course of their existence and, if so, when?

9. How are electronic records scheduled?

10. Who should be responsible for appraising electronic records?

The third domain aims to develop methods, procedures and rules for the preservation of electronic records according to the requirements identified in domain one, and to define the responsibilities for implementing them. The research questions are:

1. What methods, procedures and rules of long-term preservation are in use or being developed?

1.1. Which of these meet the conceptual requirements for authenticity identified in Domain I?

1.2. Which methods of long-term preservation need to be developed?

1.3. Which of these methods are required or subject to standards, regulations and guidelines in specific industry or institutional settings?

2. What are the procedural methods of authentication for preserved electronic records?

2.1. In what way can archival description be a method of authentication for electronic records?

2.2. In what way can appraisal and acquisition/accession reports be constructed to allow for the authentication of electronic records?

2.3. What are the procedures for certifying electronic records when they cross technical boundaries (e.g., refreshing, copying, migrating) to preserve their authenticity?

3. What are the technical methods of authentication for preserved electronic records?

4. What are the principles and criteria for media and storage management that are required for the preservation of authentic electronic records?

5. What are the responsibilities for the long-term preservation of authentic electronic records?

The fourth domain aims to develop a framework for the formulation of strategies, policies and standards. The research questions are:

1. What principles should guide the formulation of international policies, strategies and standards related to the long-term preservation of authentic electronic records?

2. What should be the criteria for developing national policies, strategies and standards?

3. What should be the criteria for developing organizational policies, strategies and standards?

The group of researchers works by means of task forces whose composition cuts across the various teams and is based on specific competence on the subject matter and different disciplinary background. Thus, for example, within the task force dealing with the first domain, computers engineers are working together with diplomatists and archival and legal experts to analyze all the technological components of each type of system and their specific function, and to study the impact that a change in each of those components would determine in the form of records made, received and/or maintained and used in the system. The consequences of physical and architectural changes, parametric changes, source changes, and format changes are looked at for the specific purpose of establishing what elements of form conditioned by the digital system are integral part of the meaning of the record and need therefore to be protected from manipulation and across migrations. While electronic engineers have much to learn from records experts about the nature of records, it is quite clear that the latter have as much to learn from the former. For example, for a long time archivists have considered e-mail to be a record form; this was found astonishing by engineers who, free from the prejudices of archival formalism, have no doubt about the fact that e-mail is only a method of transmission, just like a fax or a courier: any type of information can be transmitted through e-mail and what we see in its header is just a record of transmission, like the printed line on top of a fax or a piece of paper stuck over a courier package.

The research methodologies used are as varied as the disciplines involved in the research. Surveys, case studies, diplomatic analysis, and modeling are some of them. Preliminary findings are tested and the results communicated to the task forces. After the appropriate revisions, they are submitted to the international team for further refinement, and then tested again. To ensure consistency within the task forces and among testing sites, training seminars are regularly conducted, during which the researchers learn how to carry out the case studies so that results are comparable as to substance and form, how to use the modeling techniques appropriate to each purpose, how to test proposed methods and procedures, etc. A glossary defining all the terms used in the research also contributes to clear communication among the researchers and between them and those to whom the findings are disseminated. To guarantee that research results will be valid in each jurisdiction involved in the research, test sites are in all countries involved in the research and belong in both the public and private sector. Notably, ten national archival institutions participate in both the development and the testing of the findings.

The contextualization of the findings is vital to the success of this research project and is the primary reason for the existence of national and multinational teams within the larger international team. Their task is to take the results of the work of the task forces and examine them in the context of the administrative, legal and social systems of each country. In fact, while the project aims to formulate the universal principles, concepts and criteria that must guide the articulation of strategies, policies and standards, these must be viable and

implementable within each nation. This does not mean that the requirements for authenticity must reflect the legislation that in each country establishes procedures and norms for authenticating records. While authenticity is a quality of the record, authentication is only a means of proving that a record is what it purports to be at a given moment in time. Authentication, in other words, is a declaration of authenticity in time resulting either by the insertion or the addition of an element or a statement to a record, and the rules governing it are established by legislation. The requirements for the continuing verifiable authenticity of records go much beyond legislated means of authentication and even juridical principles and structures, deriving from the historical stratification of traditions, uses, attitudes, and perceptions that each culture brings to bear on what it treats as an authentic record. This is the reason why contextualization of the requirements identified for the authenticity of electronic records is essential to the success of the research project.

At this time, political decision-makers are very much concerned with authentication of electronic records rather than with their continuing authenticity, as shown by the increasing number of laws related to digital signatures and other similar means of proving both the authorship of a record and its integrity when received by the intended addressee. Not much interest has been directed to the preservation of such integrity over time, in such a way that it can be ascertained by anyone who has a need to access electronic records many years from now, after they have been moved across several generations of technology. Yet, administrative transparency, historical accountability, and long term legal requirements cannot be met and might actually be obstructed by authentication measures. For this reason, it is vital that political decision-makers begin looking beyond the present and considering the political, social and economical implications of the issues studied by the InterPARES research team.6

1 Armstrong v. the Executive Office of the President. U.S. District Court for the District of Columbia. 810 F. Supp 335 (DDC 1993). Friedman, Paul L. Court Opinion Transcript. U.S. District Court for the District of Columbia. Civil Action No. 96-2840 (PLF). October 22, 1997.

2 [Canada], Dishonoured Legacy: The Lessons of the Somalia Affair. Report of the Commission of Inquiry into the Deployment of Canadian Forces to Somalia, vol. 5 (Ottawa: Minister of Public Works and Government Services Canada, 1997), 1218-1219.

3 See Duranti, Luciana and MacNeil, Heather. ÒThe Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project. Ó Archivaria 42. 1996. pp. 46-67.

4 The measures described are among several other findings of the research project. All findings are summarized on the project website: http://www.slais.ubc.ca/users/duranti/

5 The direction of the research and its infrastructure are funded by the Social Sciences and Humanities Research Council of Canada (SSHRCC), and by the Hampton Fund of the University of British Columbia (UBC) and the UBC Vice President Research Fund and Dean of Arts Fund. The national and multinational research teams are funded by national granting agencies and institutional and organizational contributions. For example, the Canadian team is funded by SSHRCC and the American team by the National Historical Publication and Records Commission (NHPRC).

6 The web site of the InterPARES project is http://www.interpares.org/