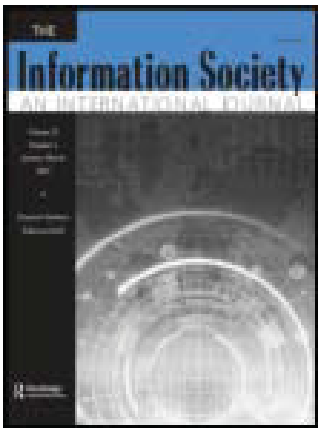

The Information Society: An International Journal
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/utis20

Concepts, Principles, and Methods for the Management of Electronic Records

Luciana Duranti

Version of record first published: 19 Jan 2011.

To cite this article: Luciana Duranti (2001): Concepts, Principles, and Methods for the Management of Electronic Records, The Information Society: An International Journal, 17:4, 271-279

To link to this article: http://dx.doi.org/10.1080/019722401753330869

The Information Society, 17:271–279, 2001

0197-2243/01 $12.00 + .00

Concepts, Principles, and Methods for the Management of Electronic Records

Luciana Duranti

University of British Columbia

This article discusses the problems and issues that have arisen with the widespread use of digital technology in the modern office, in particular those related to the trustworthiness of electronic records and to their permanent preservation. It defines the concepts of record reliability, authenticity, and authentication; it outlines the principles that should guide the creation and management of reliable electronic records and the maintenance and preservation of authentic records; and it describes methods for the management of trustworthy electronic records in the context of two research projects undertaken by the archival scholars of the University of British Columbia, the first of which, known as the UBC-MAS project, was completed in collaboration with the U.S. Department of Defense in 1994–97, and the second of which, known as InterPARES, is a multinational multidisciplinary collaboration begun in 1999 and nearing the completion of its first phase.

The widespread use of digital technologies by individuals and organizations in the usual and ordinary course of their activities is generating more information than in any previous decade of human activity. The majority of this information, however, is less reliable, retrievable, or accessible than ever before. Idiosyncratic software systems generate, manage, and store digital data using proprietary technologies and media that are not developed to segregate different types of information, to prevent manipulation or tampering, or to establish and maintain an intellectual order, and that are subject to the dynamism of the computer industry. The digital information produced by and maintained in most of the systems presently used cannot be considered trustworthy and is easily lost in a self-perpetuating and expensive cycle of obsolescence and incompatibility.

Received 24 May 1999; accepted 24 August 1999.

Address correspondence to Luciana Duranti, Chair and Professor, Master of Archival Studies, University of British Columbia, 831-1956 Main Mall, Vancouver, BC V6T 1Z1, Canada. E-mail: Luciana@interchange.ubc.ca

Moreover, organizations and individuals produce data in a variety of media and formats. It is quite common for recorded information relevant to a single matter to exist partly in a paper file, partly in an e-mail box, and partly in a spreadsheet application or in a relational database. It is essential to establish explicit intellectual links among these data at the moment in which they are created, and to maintain them while they are actively used. It is equally important to preserve such links once the records have exhausted their usefulness for the purposes for which they were generated but need to be preserved over the long term, sometimes permanently, for reference, for research use, or because of legal requirements. In fact, information is meaningless out of context, and several decades from now, users of all kinds must be able to see the entire dossier relating to the matter they are exploring.

Ad hoc attempts have been made by individual organizations to either generate all information in a single medium or transfer it to one medium of choice. For example, offices have established routines for printing out e-mail and inserting it in a paper file, scanning paper documents into electronic systems, or converting electronic and paper records to microfilm. These attempts have been unsuccessful for a number of reasons. First, both the imposition of one medium of communication on the operations of an organization and the constant conversion of material made or received in a variety of media to one medium of choice, if not required by the business at hand, hamper the workflow of the office, and their implementation tends to be sporadic and inconsistent. Second, some types of digital information do not lend themselves to conversion to a different medium. For example, hypertext cannot be printed out to paper, and scanned maps or photographs are not always reliable surrogates of the paper originals. Third, court decisions have rejected the practice of converting electronic documents to other media on the grounds that the output of such process lacks elements critical to their use as evidence.[1] For example, the printout of an electronic spreadsheet will not contain the formulas on which calculations are based.

The effects of the adoption of information and communication technologies without forecasting and planning for the consequences of hybrid systems, digital environments facilitating manipulation of data, media and digital obsolescence, and the proprietary and idiosyncratic nature of applications have already been witnessed in governments and other organizations. For example, in Canada, in the spring of 1996, the inadequacy of procedural mechanisms for ensuring the authenticity of electronic data 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 Operation 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 Forces' theatres 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 to bypass the awkward system. Therefore, the commissioners concluded that NDOC logs were not a reliable record of transactions at the operations center either for present investigators or for future researchers.

In another 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 labor 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 files of East Germany are lost to the unified German government that needs the information they contain for administrative purposes, to the citizens whose interests are implicated in those files, and to present and future researchers the world over.

Although physical preservation is an issue with digital material, it is not the major issue. The greatest challenge with which digital systems present us is the creation and maintenance of reliable data and the preservation of their authenticity over time. Moreover, this problem is most serious not with regard to electronic data or information or documents, but with regard to electronic records. *Records are defined as documents* (i.e., recorded information) *created* (i.e., made or received and set aside for action or reference) *by a physical or juridical person* (i.e., an individual or an entity capable of rights and duties) *in the course of a practical activity, as a means and instrument for it*. It is vital for every organization that its records be able to stand for the facts they are about, that is, that *their content is trustworthy*. It is equally important that, in time, those records can be proved to be what they purport to be, immune from any sort of tampering and corruption, that is, that *they are trustworthy as records*. The former type of trustworthiness is called *reliability*; the latter is called *authenticity*.

A record's reliability depends on the degree of completeness of its form[2] and on the degree of control exercised over its procedure of creation. The latter includes the control exercised over the author, who must be competent for issuing the specific record, that is, must have both the authority and the capacity to do so, and who must be responsible for the recording of the message in the record. A record's authenticity depends on its mode, form, and state of transmission,[3] and on the manner of their preservation and custody. In order to establish the terms of reference and parameters for the development of strategies, procedures, and standards ensuring the reliability and authenticity of electronic records, it is essential to be able to segregate electronic records from other forms of digital information. For the purposes of this article and in the context of the research projects discussed in it, *an electronic record is a record made or received and set aside in electronic form*. In other words, a fax transmitted electronically but received and set aside in paper form is a paper record, and so is a paper letter scanned into a computer but filed in a paper file.

To segregate electronic records from, for example, electronic documents in a document management system, it is essential that the system be able to recognize them. Thus, one needs to define the components of a record that make it different from any other aggregation of data and to do so in a way that is independent of the type of record and its specific context. An electronic record has been defined in a decontextualized way by identifying and defining its necessary and sufficient components in the course of a research project carried out in 1994–1997 by researchers of the University of British Columbia and the Department of Defense of the United States, entitled "The Protection of the Integrity of Electronic Records."[4] The necessary and sufficient components of an electronic record were found to be 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.

- *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.
- *Context*, that is, the juridical, administrative, procedural, and documentary framework in which the record is created.

The fundamental difference between electronic and traditional records is that the components of the former ones may reside in different parts of the medium or even of the system and may not physically exist if not purposely generated. This means that a complete record is one whose components have been inextricably and irreversibly linked to each other and have been made explicit by transforming them in an element of form, for example, by expressing the archival bond in a classification code.

Another difference is in the multiple manifestations of individual elements of form. For example, in an electronic record, one may have several dates: the date given to the document by its author, which demonstrates the relationship between the author of the record and its content; the date and time of transmission to either an external or an internal addressee, which represent the moment in which a record begins to have consequences; the date and time of transmission to the file or the class to which the record belongs, which reveals the development of the matter; and the date and time of each retrieval, which show every act of consultation. Each and every one of these dates may be necessary to prove either the reliability of the record or its authenticity over time.

A similar situation exists with regard to the signature, which assigns responsibility for the record and its content. A handwritten or typewritten name may be attached to a record by its author or writer, but in an electronic record it does not have the function of a signature. Instead, the name appearing in the header of an electronic mail message or in the profile of other types of record may be able to fulfill the signature function. A mix of accountability and authenticating functions is then exercised by the digital signature, that is, a digital data file that uses a computationally unique string of numbers and enables the detection of unauthorized modifications to the contents of a record. This element is not a signature but, for all intents and purposes, a seal, which is attached to the record after its completion and which, once used for the verification of the provenance and integrity of the record, has fulfilled its function.

These two examples of the date and the signature show that the control exercised by an organization on its procedures of records creation must get down to the prescription of the formal elements to be introduced in the record and kept intact for the record to be considered reliable. Thus, in addition to the traditional body of rules governing the making, receiving, routing, annotating, and setting aside of records, additional requirements must be introduced for the specific control of electronic records, aimed to ensuring their reliability, such as:

- Compiling records according to predefined standard formats and templates.
- Authenticating records using preestablished 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 "workflow rules" 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, fingerprints, etc.
- 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.

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 help 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.

In fact, another key difference between electronic and nonelectronic 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 (i.e., copying them to a new medium presenting the same technological characteristics) and periodic migration (i.e., transferring them from one hardware/software configuration to another or from one generation of digital technology to another). Refreshing generates a complete

reproduction of both the content and the formal elements of the records; therefore, the resulting records may be considered faithful copies of the original records. Migration, on the contrary, generates a reproduction of the content of the record, with changes in configuration and format, often with a ripple effect on other components of the record. Thus, migration always involves 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 form, while in others they are not and exist either as metadata or as rules that condition, for example, the records' performance. Thus, it is 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 that are not visible to the user can be made visible and stabilized by bringing them into the 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 nondigital form (e.g., microfilm); and fourth, to adopt self-authenticating and well-documented procedures for migration and an uninterrupted line of physical custody.

The latter is undoubtedly 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 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 the long term 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. 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, it is clear that there will not be much worth preserving if the individuals and organizations who produce records using digital systems do not take drastic measures to establish strong controls on records creation.

The first such measure consists of embedding procedural rules of records creation in an organization-wide, centralized records system, and of integrating business and documentary procedures. The centralized records system must include a record-keeping system and a separate record-preservation system, in order to ensure an optimum amount of control over record creation, handling, and preservation. The integration of business procedures with documentary procedures strengthens this control by identifying all the business procedures within each organization's function; breaking them down into phases; and determining for each phase the component actions, the records that must be used in relation to each action, the records that must be made, received, and handled during each action and by whom, the way in which the records have to be classified, audited, and disposed of, their level of confidentiality, and the specific methods for ensuring their reliability and authenticity.

The second measure for guaranteeing the trustworthiness of electronic records consists of instituting procedures for strengthening their interrelationships and the links that they have with the nonelectronic records created by the same organization. The tightening of these links may occur by assigning a classification to each record that makes explicit and permanent its relationship with the action in which it participates and with all previous and subsequent records resulting from the same activity. Also registration, by providing evidence of the incoming and outgoing records, freezes and perpetuates the network of documentary relationships that best serves to attest to the integrity of a record. The creation of a record profile for each record of the organization, electronic and nonelectronic, accomplishes a very similar purpose, by incorporating in an electronic form inextricably linked to the record for as long as the record exists all the metadata that uniquely identify the record and reveal what it is all about.

The third and final measure for ensuring the trustworthiness of electronic records is the integration of the management of the electronic and nonelectronic records belonging in a hybrid records system. This integration may be implemented by creating an electronic record profile for every record, electronic and nonelectronic, made or received and set aside in the central records system and by establishing a repository for those records profiles.[5]

If individuals and organizations succeed in establishing control on records creation according to the basic principles just outlined, the issue of long-term preservation of the electronic records so created will be easier to address once international policies, strategies, and standards concerning methods of preservation will have been established. At this time, there is no international consensus on the methods for protecting the integrity of the

electronic records that must be preserved indefinitely or even permanently by organizations or archival institutions and for enabling the verification of their authenticity overtime. Therefore, an interdisciplinary and international team of researchers has been assembled to address these preservation issues in a systematic 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.[6] It is directed by this author and carried out by national and multinational research teams from various countries, including, among others, Canada, the United States, England, Ireland, Sweden, the Netherlands, Finland, Germany, France, Portugal, Italy, Australia, Hong Kong, and China.[7] A global industry team includes multinational companies in the pharmaceutical, biochemical, health, and computer fields.

The research project is divided in four domains. The first domain aims to identify the requirements for preserving authentic electronic records. The second domain aims to establish whether, in order to satisfy the requirements for authenticity identified in domain one, the selection criteria and methods for electronic records need to be revised or even radically changed. 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 fourth domain aims to develop a framework for the formulation of strategies, policies, 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, such as, besides archival science, computer engineering, law, diplomatics, and music theory.

The basic concepts that constitute the theoretical framework of the project are those adopted and/or developed in the course of the previous project on the preservation of the integrity of electronic records while they are still necessary to the creator for carrying out its business.[8] They are the concepts of authenticity and reliability, and the concepts of record and electronic record, as defined earlier. Each of these concepts subsumes many other concepts, such as those related to the components of a record.

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. For those who are not familiar with the two latter methods, I next explain briefly what they are. Diplomatic analysis is the method of inquiry used by a science developed in the 17th century, diplomatics, the main purpose of which has been, over the centuries, to assess the authenticity of records of unverified provenance, independently of their context. For this reason, it is especially useful for identifying commonalities between and among types of records and records systems where they are not readily apparent, and for developing standards.[9]

Modeling methodology consists of two parts, one graphically representing the activities involved in each hypothesis and the other the entities involved in each activity. The representation of the *activities* is done by decomposing them hierarchically at as many levels as needed and identifying for each activity at every level (1) what guides or regulates it, (2) what is used to perform it, (3) what initiates it, and (4) what results from it. These four things are *entities*, which we then represent in different models by identifying their *attributes* or *characteristics* and their *relationships* one to another, on the basis of the theory and methods of diplomatics. To support the modeling process, every activity, entity, attribute, and relationship named in the models must be consistently and rigorously defined in an interdisciplinary international glossary.[10]

Preliminary findings are tested by archival institutions and industry test sites 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. The 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, 10 national archival institutions and several companies 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.

As mentioned earlier, the research is carried out by means of three task forces (on authenticity, preservation, and appraisal) and one committee (for the glossary). At this time, the Authenticity Task Force is looking in a detailed way at a large variety of electronic systems following an hierarchy of growing complexity, from systems regarded as simple databases, to document management systems, to systems containing sensory presentations (i.e., digital objects that are performed, such as music and film, or rendered on screen as images).[11] For example, the group of researchers at the University of British Columbia focuses its analysis on computer music, and includes, besides archival and diplomatic theorists, specialists from the schools of music, computer science, and computer engineering. Computer music is a very important area, not only because of the issues affecting the specific industry and mostly deriving from systems incompatibilities and obsolescence, but especially because sound accompanies more and more types of electronic records, and any requirement for authenticity that is valid for computer music would allow for the verification of the authenticity of any other type of record that is accompanied by sound.

The primary product of the work of the Authenticity Task Force will be an electronic records typology with conceptual requirements for authenticity defined for each record type. To populate the electronic records typology, the task force will perform an analysis of the empirical data gathered during the case studies.

The primary instrument that is used to analyze case study data is the *Template for Analysis*. This template was created by the Authenticity Task Force using the components of a record listed in the first part of this article. The template elements were then refined and expanded by utilizing the InterPARES International Team's combined knowledge and experience with types of electronic records and electronic systems. To further refine the template as well as to construct the electronic records typology that will be based on it, a form of grounded theory is being used. Grounded theory is a method for discovering concepts and hypotheses and developing theory directly from the data under observation.[12] Cases are selected for study "according to their potential for helping to expand on or refine the concepts or theory that have already been developed. Data collection and analysis proceed together."[13] Because a grounded theory is used, theoretical rather than statistical sampling is applied in the selection of the case studies. The process of theoretical sampling is "a process of data collection for generating theory whereby the analyst jointly collects, codes, and analyzes his data and decides what data to collect next and where to find them, in order to develop his theory as it emerges."[14] Accordingly, criteria for selection have been developed, which will evolve as case study data are analyzed. Not all case studies will respond to all the criteria listed next, but each case study should respond to at least three of them. The members of the various research groups prepare lists of systems candidates for analysis and their brief descriptions, including which criteria they meet and why. The Authenticity Task Force selects case studies from the lists in such a way that there is sufficient variety, but at the same time there is a certain number of similar systems that can be compared, and determines the schedule on which each case study will be conducted (i.e., first, second, third or fourth round). The criteria are:

1. Systems that contain, generate, or have the potential or possibility of generating records.
2. Systems that have gone through one or more migrations.
3. Systems where migration(s) was (were) from one electronic system to another electronic system.
4. Systems for which several aspects of technological context (storage media, system software, application software, data format, schema) were changed in the course of each migration.
5. Systems for which the premigration and the postmigration versions are available and are up and running.
6. Systems for which detailed documentation (design, implementation, metadata) exists.
7. Systems with a diversity of information configurations (e.g., they contain both text and images).
8. Among the candidate systems proposed by the same archival institution, an effort should be made to ensure diversity in content and type of records.
9. Between institutions, an effort should be made to identify and conduct case studies on record-keeping systems performing similar functions (e.g., student registration systems in different universities).

The Preservation Task Force has begun modeling the preservation activity and, in the process, it has clarified some fundamental properties and behaviours of electronic records. According to the preliminary report of the task

force chair,[15] the first clarification is that it is not possible to preserve an electronic record; it is only possible to preserve the ability to reproduce an electronic record.

> It is always necessary to retrieve from storage the binary digits that make up the record and process them through some software for delivery or presentation. Analogously, a musical score does not actually store music. It stores a symbolic notation which, when processed by a musician on a suitable instrument, can produce music. Presuming the process is the right process and it is executed correctly, it is the output of such processing that is the record, not the stored bits that are subject to processing . . . .
>
> Starting from the inevitable requirement to reproduce an electronic record, we can stipulate that demonstrating the authenticity of electronic records depends on verifying that (1) the right data was put into storage properly, (2) either nothing happened in storage to change these data or alternatively any changes in the data over time are insignificant, (3) all the right data and only the right data were retrieved from storage, (4) the retrieved data were subjected to an appropriate process, and (5) the processing was executed correctly to output an authentic reproduction of the record. Verifying that these technical requirements were satisfied is necessary, but not sufficient, to demonstrate the authenticity of an electronic record. It is obviously necessary because if any of these conditions is not satisfied, the result of the processing of retrieved data cannot be (asserted to be) the same as the electronic record from which the stored data were produced. It is not sufficient because there is nothing in it that applies specifically to a record. It would be accurate, then, to say that this technical verification is a method for demonstrating that a digital object produced from stored digital data is an authentic reproduction of a digital object that was stored. To be precise, we should not even refer to "a digital object that was stored," but to the digital object that was the source of the stored data.[16]

To move beyond the general class of digital objects to the more specific class of electronic records, we must apply criteria that specifically relate to authentic records. These criteria, that is, the requirements for ensuring the authenticity of electronic records, will result from the work of the Authenticity Task Force, but there is a substantial amount of analysis that the Preservation Task Force must do even before the findings of the Authenticity Task Force are available. It will have to study and represent by means of models situations that present identifiable risks of changing the records. These situations can be described as *boundary conditions*: "A boundary condition is a state from which a record cannot be moved without either changing the record itself or taking some action either to prevent the threatened change or to counteract or to compensate for it."[17] There are categories of boundary conditions: for example, the conditions generated by the processing of records, when the activities involved in it entail some risk that the records be altered; the conditions created by the technology dependencies of the records, when the activities involved in altering the dependency or the technology, or removing the records from them, imply changes in the records; and the conditions that derive from the transfer of the physical and legal custody of the records from the creator to the preserver.

The Appraisal Task Force has completed an analytic review of the literature concerning the selection of electronic records. Subsequently, it has acquired from several archival institutions that have received from the creator physical and legal custody of electronic records the related appraisal reports. An examination of these and of the case studies results[18] has prepared the foundation for the modeling effort of the selection process that has just begun. The research questions that the Appraisal Task Force aims at answering are:

1. What, if any, is the influence of digital technology on selection criteria?
2. In what ways does appraisal for selection 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 selection?
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 and selected?
8. Should electronic records be appraised and selected 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 assumption here is that, independently of selection criteria, the process of appraisal will have to be quite different from the existing one if we want to be able not only to maintain the records as reliable as they were when created and authentic, but also to verify and certify their authenticity over time. In other words, once the Authenticity Task Force will have determined the requirements for authenticity for the various types of electronic records, the Appraisal Task Force will have to identify a process capable of respecting such requirements.

The Glossary Committee is the fourth unit of research and in a way the organ that is primarily responsible for the conceptual integration of the work of the task forces. The major issues raised by international interdisciplinary collaboration derive from the different use made of the same term in the various disciplines and by the use of

different terms to refer to the same entity or activity among the various countries. These are both scientific and cultural issues that need to be brought forward and dealt with in a scholarly analytical way, so that they may be overcome by a profound understanding of all concepts and traditions involved, rather than by compromise, which in the end would not satisfy anyone and would not serve the research project.

The Glossary Committee is composed of a member of each task force, a neutral chair, and the project director. Three students research assistants do the research work for it. The committee receives nominations of terms for the glossary with one or more proposed definitions from the task forces, through the task force representative in the committee, or from the project director (especially if the term is formally used in one or more InterPARES documents). The research assistants research the term and its definition through time and across disciplines, and then submit the outcome to the committee. Discussion follows and then a vote for the inclusion or not of the term with its definition(s) in the official glossary of the project, which must be unanimous. If unanimity is not reached, the term in question and related definition(s) are sent back to the unit that proposed it (i.e., a task force or the project director) with comments and recommendation. To ensure internal consistency of the glossary, it is inevitable that terms and definitions already included in it be revisited in light of new terms and definitions proposed and developed by the task forces in the course of their work. It is the shared responsibility of the committee and the task forces to monitor consistency and to either solicit or submit proposals of changes to already approved terms.

The InterPARES research has begun in stride and reached a good momentum. From now on one can expect increasing activity and results. The research teams will endeavor to communicate them on a regular basis to both the record and information-related professions and the community at large through conferences, talks, articles, and the project's web site. While it is quite clear that, although there will be findings on a continuing basis, this research will never yield definitive solutions to the problems presented by electronic records, given the increasing pace of technological development, it is essential to understand that its primary aim is and should be the formulation of the principles that must guide the development of international, national, and organizational policies, strategies, and standards, the specific criteria for each type of policy, strategy, and standard, and the procedural methods for their implementation. The most important thing is to ensure that the policies, strategies, and standards are consistent with one another, and this is only possible when they are inspired by the same principles.

Everything we have learned so far about electronic records reinforces the idea that any technological as well as procedural method of management in general and preservation in particular will need to be based on a clear and detailed articulation of concepts and formulation of principles, and that specific choices will have to derive from the interpretation and careful application of those same concepts and principles in light of a deep understanding of the context in which they will have to be made. As the draft report on the Universal Preservation Format states, "The integrity of digital information is a moral issue,"[19] but it is also a political and economic one, and it is essential to make such issue as independent as possible of the whims of governments and the interests of the industry if we want to have any hope that the generations to come will receive a trustworthy record of their past.

> In 1977, two Voyager spacecraft left Earth on a mission to explore and send back information about our solar system and beyond. Attached to each vehicle was a gold-plated phonograph record which contained 115 images, a collection of Earth's natural sounds, greetings in 55 languages, and samples from the like of Bach, Beethoven, and Chuck Berry. Each record included a stilus, and inscribed on its protective aluminum jacket were visual instructions on how to play it. The disks were intended by Carl Sagan and his team of managers and engineers as a kind of packaged time capsule for any aliens or distant cousins who, several centuries from now, may be rocketing along.[20]

Although very evocative, the idea that the only way of transmitting the authentic recorded residue of our times and deeds to the next generations is to load it on a spacecraft, complete with a self-described mechanism, seems to deprive the concept itself of cultural documentary heritage of its meaning and purpose. Whose culture, whose heritage, if we are not active participants in a constant process aimed to salvage, protect and rebuild it, to select, refine, and identify it, and to reproduce, challenge, and verify it? Our intellectual effort to carry forward our past as well as our present is an integral part of the record of our time and contributes to its contextual meaning and to its significance. It is a work of love that tells better than anything else what we value the most.

NOTES

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

2. The form of a record comprises the rules of representation according to which the content of a record, its administrative and documentary context, and its authority are communicated. It possesses extrinsic and intrinsic elements. The former elements are those that determine the material makeup of the record and its appearance (e.g., language, presentation features, special signs, seals). The latter elements are those that convey the action in which the record participates and its

immediate context (e.g., names of author and addressee, dates, place, subject, description of action, corroboration, attestation). Documentary form also includes annotations, that is, additions made to the record after its completion, either in the course of executing it (e.g., indication of attachments, authentication of signatures, priority of transmission), in the course of handling the matter to which the record relates (e.g., date and time of receipt, name of handling office, date and time of further action or transmission), or in the course of managing the record for records management purposes (e.g., classification code, registration number).

3. The mode of transmission is the means used to communicate the record (e.g., regular mail, e-mail, fax). The form of transmission is the way in which a record is received or, if it is an internal record, set aside within the record system (e.g., on paper, as a digital object). The state of transmission is the degree of completion of the record when it is set aside for use or reference (i.e., the record is a draft, an original or a copy).

4. The project has produced the Department of Defense's records management standard for electronic records systems. For a summary of the findings of the project and the definitions of all the necessary and sufficient components of a record, see Duranti, Luciana, and MacNeil, Heather, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project." *Archivaria* 42, 1996, pp. 46–67. For additional details, see the project web site ⟨www.slais.ubc.ca/users/duranti/⟩.

5. The measures described are among the findings of the research project on the "Protection of the Integrity of Electronic Records" mentioned earlier.

6. 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).

7. The national teams are the Canadian, American, Australian, and Italian research teams. The multinational teams are the European, Asian, and Global Industry research teams. In the course of this first year of the research, multinational teams are still open to the participation of additional members. For example, the Asian team may be joined by Japan and Korea. The names of the individual scholars involved, with their institutional affiliation, and of the participating organizations/institutions, can be found on the project web site: www.interpares.org.

8. See Duranti, Luciana, and MacNeil, Heather, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project," cited earlier.

9. Those who are interested in learning more about diplomatics, may read: Duranti, Luciana, *Diplomatics: New Uses For an Old Science*. Chicago, Il: SAA, ACA, and Scarecrow Press, 1998.

10. The primary modeling methodology used by the InterPARES group is IDEF. For a description of this methodology, see http://www.idef.com/overviews/idef0.htm and http://www.dtic.mil/c3i/bprcd/0050/tsld001.htm.

11. This categorization has been made in an unpublished paper written by Clifford Lynch for a workshop on authenticity held in Washington. DC on January 22, 2000 by the Council on Library and Information Resources, and entitled "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Dominant Role of Trust." He discusses data, documents, sensory presentations, and interactive works.

12. Glaser, Barney G., and Strauss, Anselm L., *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Atherton, 1997, pp. 6–7, 46.

13. Taylor, Steven J., and Bogden, Robert, *Introduction to Qualitative Research Methods: The Search for Meanings*, 2nd ed. New York: Wiley, 1984, p. 126.

14. Glaser and Strauss, p. 45.

15. The chair of the Preservation Task Force is Ken Thibodeau, from the National Archives and Records Administration of the United States. The chairs of the Authenticity and Appraisal Task Forces are respectively Heather MacNeil and Terry Eastwood from the University of British Columbia.

16. From the preliminary report of the chair of the Preservation Task Force, 31 March, 2000.

17. *Ibidem*.

18. It is important to note that the questionnaire guiding the semistructured interviews used in the case studies include several questions the answer to which has significant consequences for the appraisal of the records generated and/or maintained in the system in question.

19. MacCarn, Dave, and Shepard, Tom, *The Universal Preservation Format*. Draft document revised 29 December, 1998, p. 24. Circulated through the Electronic Records (ERECS-L) listserv.

20. *Ibidem*.