A LITERATURE REVIEW OF AUTHENTICITY OF RECORDS IN DIGITAL SYSTEMS
FROM 'MACHINE-READABLE' TO RECORDS IN THE CLOUD
REVISÃO DE LITERATURA SOBRE A AUTENTICIDADE DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS
DA 'MACHINE-READABLE' AOS ARQUIVOS NA NUVEM

Corinne Rogers, PhD | Professora adjunta de diplomática e de documentos arquivísticos forenses, na University of British Columbia, Canadá. Coordenadora do Projeto InterPARES Trust

RESUMO

Este artigo apresenta uma revisão de literatura sobre a autenticidade de documentos arquivísticos, partindo dos fundamentos teóricos, de maneira a embasar os textos atuais sobre autenticidade dos documentos arquivísticos digitais. O corpo principal da literatura considerada fundamenta a disciplina arquivística europeia, norte-americana e australiana, no que se refere a questões de autenticidade na produção, gestão, uso e preservação de documentos e dados (em qualquer meio).

Palavras-chave: autenticidade; documentos arquivísticos digitais; preservação; InterPARES; diplomática.

ABSTRACT

This paper presents a review of the literature about authenticity of records, beginning with the foundational theoretical literature in order to frame current writing on authenticity of digital records. The main body of literature considered that is the foundation of the European, North American, and Australian archival discipline, as it relates to issues of authenticity in the creation, management, use, and preservation of records and data (regardless of medium).

Keywords: record authenticity; digital records; preservation; InterPARES; diplomatics.

RESUMEN

En este artículo se presenta una revisión de la literatura acerca de la autenticidad de los documentos de archivo desde los fundamentos teóricos, con el fin de embasar los textos actuales acerca de la autenticidad de los documentos de archivo digitales. Grande parte de la literatura considerada fundamenta la archivística europea, de la América del Norte y Australia en cuanto se refiere a las cuestiones de autenticidad, producción, gestión, uso y preservación de documentos y datos (independientemente del soporte).

Palabras clave: autenticidad; documentos de archivos digitales; preservación; InterPARES; diplomática.

INTRODUCTION

The concept of authenticity of records is fundamental to archival science, and enjoys a centuries' long theoretical foundation. Sir Hilary Jenkinson believed that archival documents (i.e. records) were "authenticated by the fact of their official preservation" (Jenkinson, 1937, p. 4). To Jenkinson, records' history of legitimate custody alone was a sufficient predictor and guarantor of the trustworthiness of the material. However, the relative archival utopia of the pre-World War II era was short-lived as the volume of material destined to enter archives exploded. Writing 50 years later, Michael Cook dismissed Jenkinson's absolute faith in the documentary chain of custody (or perhaps the assumption that such chain of custody could be presumed or demonstrated): "We no longer believe, as Jenkinson did, that an archive's value in research or as legal evidence depends on our certainty that it has never left official custody" (Cook, 1986, p. 129). Thus, archival institutions cannot trust the records they intend to acquire solely on the basis of their custodial history, but must test them for indications of their authenticity through studying their provenance and elements of their form (diplomatics) (Cook, 1986, p. 7).

Digital technology has further upset the traditional systems of control that have ensured the creation of reliable records, and the means of presuming their continued authenticity over time and across technological change (Lauriault et al., 2007, p. 140; MacNeil; Gilliland-Swetland, 2005, p. 21). Digital records differ significantly from paper records. They are volatile and subject to loss, intentional or unintentional alteration, contamination, or corruption, even when they are still in the custody of their creator. Their authorship, provenance, or chain of custody may be difficult or impossible to determine. They may be transmitted, shared, and copied with ease. Their accessibility is subject to hardware and software obsolescence and incompatibility. Even if the creator relies on a digital record in the course of business, and maintains its unbroken chain of custody, the fragility and vulnerability of digital records demands explicit action to protect the record's authenticity. Furthermore, reliability and accuracy are no longer directly linked to authenticity and may be compromised together or separately (Duranti, 2005; Duranti; MacNeil, 1997; Duranti; Thibodeau, 2006; MacNeil, Gilliland-Swetland, 2005). When creators use cloud-based services, these challenges are multiplied.

Digital preservation research investigates the nature of digital objects, including records and data, and the attributes that may support the presumption of their authenticity. While much research has been and continues to be conducted into the protection of authenticity in the context of requirements for digital preservation, current means of evaluating authenticity for records professionals still do not offer quantifiable measures, and generalizable models that can reduce the problem to concrete, atomistic elements are elusive.

In 2014, I researched how records professionals approach the issue of authenticity of digital records for which they are responsible. My hypothesis was that, despite clear guidance from archival science on the means of ensuring record authenticity, a guidance reflected in the products of several large-scale, significant and influential research projects (InterPARES

Trust, 2015; Factor et al., 2009; Duranti; Preston, 2008; Duranti; Preston, 2005), the theoretical recommendations of these projects are not being consistently applied in practice, and records professionals are often unclear about how to define authenticity, how to protect it, and how to assess it (i.e. how to authenticate records and data).

In this paper I review the literature about authenticity of records that formed the basis of my research, beginning with the foundational theoretical literature in order to frame current writing on authenticity of digital records. The main body of literature considered is the English-language or English-translation corpus that is the foundation of the European, North American, and Australian archival discipline,[1] as it relates to issues of authenticity in the creation, management, use, and preservation of records and data (regardless of medium).

THEORETICAL FOUNDATIONS

DEFINING DOCUMENTARY AUTHENTICITY

The concept of documentary authenticity has ancient roots. The word derives from the Anglo-Norman, Old and Middle French, with reference to a thing (as a noun, *authenticum*, originally and frequently a legal document), or a person (as an adjective, denoting trustworthy, credible, genuine, or legally or duly qualified). Its etymon is the Latin *authenticus*, referring to documents (2nd century a.d.), persons (3rd century a.d.), and later coming to mean some*thing* or someone who is authoritative (from 8th century in British sources), or a thing that is legally valid (12th century) (Oxford English Dictionary, 2014).

According to archival theory, a record is a document made or received in the course of practical activity and set aside for future action or reference. The definition of record authenticity holds that authenticity is "the trustworthiness of a record as a record, i.e. the quality of a record that is what it purports to be and that is free from tampering or corruption" (InterPARES, 2012). The Society of American Archivists defines authenticity as: "The quality of being genuine, not a counterfeit, and free from tampering, and is typically inferred from internal and external evidence, including its physical characteristics, structure, content, and context". Authenticity does not automatically imply reliability of the content of the record (Pearce-Moses, 2005; Duranti, 1998a). ISO 15489, the international records management standard, identifies authenticity as follows: "An authentic record is one that can be proven: a) to be what it purports to be, b) to have been created or sent by the person purported to have created or sent it, and c) to have been created or sent at the time purported" (ISO 2001, section 7.2.2).

Authenticity is a critical concern in domains of history, jurisprudence, and diplomatics.

---

1 The term 'archival discipline' used includes management of current records by their creator (the records management literature) as well as ongoing use and preservation of records used also by persons or organizations other than their creator. For a discussion of the historical roots of the archival and records management disciplines, see Dollar, 1993 and Duranti, 1998b; 1998c.

For the purposes of understanding and analyzing documents and records, Duranti has differentiated three types of authenticity: diplomatic, legal, and historical.

> Legally authentic documents are those which bear witness on their own because of the intervention, during or after their creation, of a representative of a public authority guaranteeing their genuineness. Diplomatically authentic documents are those which were written according to the practice of the time and place indicated in the text, and signed with the name(s) of the person(s) competent to create them. Historically authentic documents are those which attest to events that actually took place or to information that is true (Duranti, 1998a, p. 45-46).

The concept of an authentic document is conditioned by the discipline in which it is considered – and therefore the purpose the document serves. In the digital environment, finding a common understanding of "the multiple meanings and significance of authenticity" remains critical (Clir, 2000, p. vii), and yet continues to be elusive.

TRADITIONAL ARCHIVAL THEORY

The roots of archival theory and concepts of record authenticity are anchored in legal and administrative principles, first executed in centralized public repositories of written documents, then, with the spread of literacy, expanding into the regulated recordkeeping practices of public and private organizations, administrations, and homes (Eastwood, 1994; Duranti, 1998c). Principles from Roman law that have become part of the foundation of archival knowledge include the idea that antiquity provides records with the highest legal authority, that deposit in a public place guarantees reliability of records as witnesses of actions, and that an unbroken chain of custody ensures records' continuing authenticity. The theory of the nature of archival material derives from the analysis of the relationship between records and their producing body, that body's functions and activities, and the rights and duties of the people interacting with it – related to the theory of the state at the time, designed to accomplish the purposes of the state (Duranti, 1996a). Early modern archival discourse was thus cradled in the public and state archives of Europe, articulated in the influential writings of practitioners such as the Dutch trio, Muller, Feith and Fruin, and the seminal works of English theorist Sir Hilary Jenkinson. The evidentiary capacity of records was at the core of these theories, shaping archivists' understanding of authenticity and their role in protecting probative value. Archival theory and legal notions of documentary evidence remain intertwined to this day.

Archival practice was not concerned originally with the need to establish or prove explicitly records' authenticity. Rather, authenticity was an intrinsic characteristic of records, a quality of their archival nature resulting from the circumstances of their creation, maintenance, and preservation. In his seminal work, *Manual for Archives Administration*, Sir Hilary Jenkinson noted "two common features [of records] of extraordinary value and importance" upon which "they can be analyzed and tested", namely impartiality and authenticity

(Jenkinson, 1937, p. 12). These derive from their creation (records are "drawn up and used in the course of an administrative or executive transaction (whether public or private) of which [they] formed a part") and maintenance ("and subsequently preserved in their own custody for their own information by a person or persons responsible for that transaction and their legitimate successors") (Jenkinson, 1937, p. 11). The contingencies that endow authenticity "are observable not in the document itself but in the procedures" of creation, maintenance, and preservation (Eastwood, 1994, p. 127). While the validity of Jenkinson's theory of the inherent characteristics of archives has been vigorously debated and has been rejected by many contemporary writers (e.g. Cook, 1997; 2001; McKemmish, 2001; Nesmith, 2002), it remains a valuable link in understanding the development of archival notions of authenticity. Regardless of critiques of his ideas, Jenkinson's "spirited defence of the evidential character of records certainly remains inspirational to archivists everywhere" (Cook, 1997, p. 25), and according to Duranti, protection of record authenticity, his "moral defence of archives," (Jenkinson, 1937, p. 83) remains a primary function of the archivist (Duranti, 1996b, p. 518).

DIPLOMATICS

The science of diplomatics was developed in the 17th and 18th centuries to prove the authenticity, and indirectly, the reliability, of archival documents, in order to establish the existence of patrimonial rights of the church and its religious orders and other authorities, and to identify and eliminate forgeries. Diplomatic authenticity is concerned with proving that a document is what it purports to be through the study of its creation, forms, status of transmission, its relationships with actions and persons, and with its juridical and provenancial contexts (Duranti, 1997).

In classic diplomatics, trustworthiness equates with authenticity, which implies a presumption of reliability, accuracy, and legitimacy. This inference was possible because of the highly controlled process of creation, maintenance, and preservation of the ancient documents that were the subject of study of the early diplomatists. By establishing the identity of the document, its integrity was presumed. Diplomatics developed into sophisticated system of ideas about the nature of records and has evolved to analyze and evaluate individual documents in terms of this system of formal elements, through which those documents can be shown to have been "written according to the practice of the time and place indicated in the text, and signed with the name(s) of the person(s) competent to create them" (Duranti; Eastwood, 1995; Duranti, 1998a). Authenticity is thus evaluated by establishing the document's identity and confirming its integrity. However, with digital records, identity and integrity are no longer linked. Modern diplomatics establishes the trustworthiness of a record in terms of three elements – reliability, accuracy, and authenticity, but cannot infer from that truthfulness or legitimacy.

Between 1989 and 1992, Duranti published a series of articles that explained the principles of classic diplomatics and applied and adapted them to records of modern bureaucra-

cies, extending them beyond traditional analogue records into the realm of digital records.[2] By integrating the principles and concepts of diplomatics with those of archival science, Duranti developed a conceptual model of an authentic record, regardless of medium, based on jurisprudence, administrative history, and archival and diplomatic theory (Duranti;d MacNeil, 1997; Duranti, 1998a; Duranti, 2001). Archival diplomatics, used both retrospectively (to understand the nature and attributes of existing records and to assess their trustworthiness) and prospectively (to design documentary forms and procedures and to develop trusted record-making, recordkeeping and record preservation systems), has provided the theoretical foundation for two decades of research into issues of reliability and authenticity of digital records (Duranti; MacNeil, 1997; Duranti et al., 2003; Duranti; Preston, 2005; Duranti; Preston, 2008).

EARLY ARCHIVAL CONCERNS WITH ELETRONIC RECORDS: BEFORE 1990[3]

Our familiarity and comfort with assessing the authenticity of traditional records stems from our ability to see, touch, and hold them. In the digital world, we do not see a physical document, but a display of assembled digital components – streams of bits ordered by sets of rules interacting in different layers of the technology (operating system, transport protocols, software applications, etc.) written in languages humans cannot directly read or understand.

The National Archives and Records Administration (Nara) accepted its first electronic records (mainly flat database files and ASCII records) from U. S. federal agencies in 1969. Authenticity of these electronic records was ascertained through visual inspection of printouts (Nara, 2015). In 1973 the Public Archives of Canada established a Machine Readable Archives Division, following in the footsteps of the United States and Sweden. It developed methods and standards to meet the Archives' mandate of appraisal and acquisition, processing, conservation, and public service (Naugler, 1978). It was not until 1978 that Charles Dollar called for continuing retention of electronic records, evaluated, or appraised, by a dual process of technical and intellectual considerations. Dollar considered such records to have informational value only, with no legal or business value, thus distinguishing these electronic records from traditional records in a creator's fonds (Dollar, 1978). This position was challenged in

2 Six articles, entitled Diplomatics: New Uses for an Old Science (Parts I-VI) were published in *Archivaria* over the course of six issues, providing the most comprehensive examination of diplomatics available to English-speaking audiences. In 1998, the articles were published as a book of the same title (Duranti, 1989a; 1989b; 1990a; 1990b; 1991a; 1991b; 1998a).

3 Early literature distinguished traditional paper records from "machine readable" records – those records whose form could be recognized, accepted, and interpreted by a machine, analog and digital (Dollar, 1978). As storage media evolved, the term "machine-readable record" gave way to "electronic record," a generic term defined as "an analogue or digital record that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person" (InterPARES, 2012). When talking about records created and/or stored in digital computers, the term "electronic record" has gradually been replaced by the more accurate term "digital record" (InterPARES, 2012).

1981 by the Public Archives of Canada, which called for computer-generated records to be appraised in the context of the whole of a creator's records and on the basis of the same taxonomy of values as paper records. This position subsequently gained international acceptance within the archival community following publication of the Unesco Records and Archives Management Programme (Ramp) study authored by Harold Naugler in 1984 (Naugler, 1984). This study highlighted the lack of legislative support, restrictions on transfer to archives, and the lack of programs for identifying, inventorying, and scheduling electronic records that makes their systematic acquisition difficult, if not impossible. The issue of appraisal was at the forefront of archival writing in this period; however, despite the challenges to the appraiser presented by issues of authenticity, nowhere did this literature "concern itself with the authenticity of electronic records" (Duranti, 2002).

As archivists grappled with the issues of value and application of appraisal criteria to electronic records, their legal status and the circumstances of their admissibility was also a subject of intense debate. In common law countries, case law responded slowly to the increasing use of computer records at trial, and legislation continued to adapt to reflect the new reality. Perhaps the highest profile and most influential case for archival issues concerning electronic records was *Armstrong v. the Executive Office of the President,* commonly known as the Profs case, in 1989 (MacNeil, 2000, p. 77-79; Bearman, 1993). This case raised issues concerning the essential characteristics of electronic records and the verification of their authenticity and determination of their reliability. As a result of the Profs case,

> judicial officers, administrators, systems designers, records keepers and researchers are reviewing their practices and the assumptions behind them, and searching for a) criteria that would allow them to determine when electronic records can serve as reliable evidence of action and decision, for b) techniques that would allow them to preserve such evidence intact, and for c) methods that would allow them to verify and prove its authenticity (Duranti; Eastwood 1995, p. 213).

This case served as a catalyst for several prominent research projects into issues of creation, maintenance, and preservation of electronic records, including the nature of electronic records themselves, and their reliability and authenticity.

AUTHENTICITY OF DIGITAL RECORDS: 1990 AND BEYOND

REPORTS AND POSITION PAPERS: INTERNATIONAL COUNCIL ON ARCHIVES

The authenticity of digital records emerged as a critical issue in the early 1990s (cf. Duranti; Eastwood, 1995; Duff, 1996; Duranti; MacNeil, 1997; Bearman; Trant, 1998). In 1993 The International Council on Archives (ICA) Committee on Electronic Records began developing a series of products, the goal of which was to "undertake study and research, promote the exchange of experience and draft standards and directives concerning the creation and ar-

chival processing of electronic records". Three Studies resulted from this initiative: *Electronic Records Programs: Report on the 1994/95 Survey*; *Electronic Records Management: A Literature Review*, and *Guide for Managing Electronic Records from an Archival Perspective*. *Electronic Records Management: A Literature Review* provided an "exhaustive review of the international literature on electronic records" and formed the foundation of the subsequent *Guide for Managing Electronic Records from an Archival Perspective* (Committee on Electronic Records, 1997). The *Literature Review* covered "the latest thinking and theories of leading experts in the management of electronic records" (Erlandsson, 1997, p. 12), predominantly from 1992-1996, including an extensive discussion of the issues of reliability and authenticity of digital records as they were addressed in two important research projects, the Pittsburgh Project, and the UBC-MAS Project.

The *Guide* describes the implications of electronic records management for archives from the legal, organizational, human resources and technological perspectives, and proposes strategies for operationalizing this work. Among its findings were recommendations that the archives be involved in the entire life cycle of electronic systems in which records are made or received and retained and "ensure that records creators create and retain records which are authentic, reliable, and preservable" (Committee on Electronic Records, 1997, p. 8). The *Guide* adopts the position that an organization's main purpose in creating and keeping records is to provide evidence of activities and transactions, to which end electronic records must be created reliable and preserved authentic. These twin concepts – reliability and authenticity – are the foundation of accountability (Committee on Electronic Records, 1997, p. 24). They remain so today.

At the XIVth International Congress on Archives in Seville, Spain, in 2000, the ICA formally acknowledged the importance of preserving authentic electronic records and called upon National Archivists to provide leadership. In 2001 the ICA established a working group within the Committee on Archival Legal Matters to prepare a report identifying "the issues that archivists and records keepers must keep in mind to ensure the authenticity of electronic records" (ICA, Committee on Archival Legal Matters, 2002, p. 4). The working group consulted the Committee on Electronic Records, and published its report in 2002, concluding that the preservation of authentic electronic records should be a critical priority for records professionals (ICA, Committee on Archival Legal Matters, 2002, p. 10).

The report adopts a position of jurisdictional neutrality, and embraces the definition of record authenticity put forward in the international records management standard, ISO-15489-1. The requirement for authenticity is linked to four reasons for creating archives: to prove legal rights, to serve as instruments for the administration of an organization, and to serve as cultural heritage and as one of the preconditions for social and political accountability. Authentic documents are "reliable not only at the moment when they are created but remain reliable for a long time to come" (ICA, Committee on Archival Legal Matters, 2002, p. 6).

In 2004, a second report prepared for Unesco and the ICA was published "to address the global status of authenticity of electronic records, with particular attention to developing countries". The central question asked was "what measures are necessary for records and

archives professionals, especially in developing countries, to ensure the authenticity of electronic records…" (Millar, 2004, p. 4). Challenges to authenticity were presented as recurring themes, including the low profile of record keeping, the focus on IT-oriented approaches to creation, management, and preservation of electronic records, the absence of technical or operational standards for management of electronic records, the absence of sustained educational initiatives, and the need for a strategic approach to capacity building (Millar, 2004, p. 8). The eleven recommendations resulting from the consultative exercises that addressed that question were not detailed with respect to ensuring authenticity of records (in contrast with the specific recommendations and guidelines offered by research projects such as InterPARES), but high-level strategic priorities and actions for Unesco, the profession, and the ICA to undertake in response to the identified challenges.

THE COUNCIL ON LIBRARY AND INFORMATION RESOURCES

The Council on Library and Information Resources (Clir) published a set of position papers in May 2000 by experts from different domains of the information resources community. The papers addressed the question: What is an authentic digital object? In the introduction to the collection, the authors recognized that "authenticity" in recorded information connotes "precise, yet disparate, things in different contexts and communities". The goal of the report was to bring together different communities of practice to arrive at a common understanding of key concepts and terms regarding authenticity. This involved exploring the "meaning and significance of content, fixity, consistency of reference, provenance, and context". The report published the perspectives on authenticity of five professionals: a digital librarian, a documentary editor, a special collections librarian, a document theorist, and a computer scientist, asking each to address the nature of a digital object from his/her perspective (Clir, 2000, p. vi). The view closest to that of an archivist is outlined below.

Clifford Lynch, in his contribution to the Clir report, distinguished philosophical (social) and computational (technological) constructs in determining authenticity and integrity. According to Lynch, distrust of the digital is forcing exactitude on concepts of authenticity and integrity, yet the result is abstract and elusive, defying testable definitions. Furthermore, distrust of the digital environment appears to be balanced by faith and optimism about the potential for technological solutions – the "magical arsenal [that] has solved the problems of certifying authorship and integrity" (Lynch, 2000, p. 33). Lynch highlights the role of integrity in the determination of authenticity in the digital environment, something that I found to be a pervasive theme fifteen years later. "It is an interesting, and possibly surprising, conclusion" claims Lynch "that in the digital environment, tests of integrity can be viewed as just special cases and byproducts of evaluations of authenticity" (Lynch, 2000, p. 41).

THE PRESERVATION OF THE INTEGRITY OF ELECTRONIC RECORDS – UBC-MAS PROJECT

Researchers at the University of British Columbia took a very different approach to that of the consultative reports discussed above. The Preservation of the Integrity of Electronic Records was a three-year research project (April 1994-March 1997) carried out at the Uni-

versity of British Columbia under the direction of Principal Investigator, Luciana Duranti and Co-Investigator, Terry Eastwood, and with the support of Research Assistant, Heather MacNeil.[4] One of the project's strengths was its focus on identifying and defining on purely theoretical grounds the byproducts of information systems, and protecting the integrity of records (those byproducts which constitute evidence of actions) in those systems. This distinguished it from other projects whose research foci fell within specific legal or programmatic frameworks. The premise was that the identification of the criteria, techniques, and methods needed to solve the problems posed by the use of electronic information systems for carrying out business "cannot derive from purely pragmatic or *ad hoc* decisions but must be rooted in principles and concepts that can be applied in different situations and various contexts" (Duranti; Eastwood, 1995, p. 214). The theoretical foundation was provided by principles of diplomatics integrated with principles of archival science and interpreted within the framework of electronic systems (Duranti; MacNeil, 1997, p. 47).

The researchers adopted the perspective of the records creator, specifically a corporate body. While an agency is using its records it has a direct interest in "making and maintaining reliable and authentic records in order to carry out its activities". Once the records are no longer used, that circumstantial guarantee of trustworthiness no longer exists, and transfer to a neutral third party is essential (Duranti; MacNeil, 1997, p. 57-60).

The first step of the project was to define terminology – what exactly was meant (and could be operationalized) by the terms 'integrity', 'reliability', and 'authenticity'. The precision with which these and other concepts were analyzed and defined is characteristic of the UBC project and the subsequent InterPARES projects. The meaning of the concepts of reliability and authenticity were derived from diplomatics: reliability is the authority and trustworthiness of records as proof and memory of the activity, their ability to stand for the facts they are about. Reliability can be assessed by degrees, based on the accumulated information about the level of control over the procedure of the record's creation (the body of rules governing the making, receiving, and setting aside of records, and competence of persons involved), and the degree of completeness of the record's form (that the record possesses all the elements of intellectual form necessary for it to be capable of generating consequences). Traditional indicators of reliability include one or more dates (linking the document to its author and the fact observed to its observer) and a signature (which assigns responsibility for the record and its content, and makes of the record a fact to be observed.) The more rigorous and detailed the rules and the more established the routine, the more reliable the record will be. Reliability is the sole responsibility of the creator of the record, through the record's form and procedure of creation, and the trustworthiness of the persons involved in its creation.

4 InterPARES was funded by the Social Sciences and Humanities Research Council of Canada (SSHRC). The results of the Project are available at the Project website, available in: <http://www.interpares.org/UBCProject/intro.htm#BIBLIOGRAPHY>.

A record can never be adjudged more reliable than at the moment of its creation (Duranti; MacNeil, 1997, p. 54).

Authenticity is defined as the trustworthiness of a record as a record – that it is what it purports to be and is free from tampering or corruption (Duranti, 2001, p. 44). It refers to

> the maintenance of a record's reliability through its transmission, use, and preservation over time. A record is authentic when it can be proved to be that which it is claimed to be at some point in time after its creation […]. Authenticity is provided to a record by the controls established on its transmission and preservation. In contrast to reliability, authenticity cannot be assessed by degrees: a record is either authentic or not (Duranti; Eastwood, 1995, p. 216).

Authenticity and reliability are linked in the following way: "Authenticity […] is protected and guaranteed through the adoption of methods that ensure that the record is not manipulated, altered, or otherwise falsified after its creation, that is, the record is precisely as reliable as it was when made, received, and set aside" (Duranti; MacNeil, 1997, p. 56). It was in preservation and custody that the research team found the greatest difference between analogue and digital records: while the authenticity of analogue records is protected by keeping them in the same form and state of transmission as when created and set aside, the vulnerability of digital records and rapid obsolescence of hardware and software demands that they be copied and migrated over time through "self-authenticating processes of reproduction […] and conversion" (Duranti; MacNeil, 1997, p. 57).

There were two categories of research findings: specific methods for ensuring reliability and authenticity of electronic records, and management issues concerning the maintenance and preservation of reliable and authentic records. The team found that reliability and authenticity are best ensured by embedding procedural rules in the overall records system and by integrating business and documentary procedures, and by establishing agency-wide control. Procedures that strengthen the archival bond (e.g. classification, registration, and record profiles) provide the best guarantee of reliability and authenticity, and preservation of these qualities is only possible if the management of the electronic and non-electronic components of the records system is integrated. The team recommended that the life cycle of managerial activity directed to the preservation of the integrity of electronic records be divided into two phases: control of the creation of reliable records and maintenance of authentic active and semi-active records, and preservation of authentic inactive records. A separation of duties between the records creator (who assumes primary responsibility for their reliability and authenticity while they are needed for business purposes) and the records preserver (who assumes responsibility for their authenticity over the long term) provides the best assurance of the integrity of electronic records. Reliability, governed by the creator, is ensured by procedural and technological controls over persons, process of creation, and definition of record forms. Authenticity is "guaranteed by the adoption of procedural and technological methods aimed at ensuring their proper identification in context (administra-

tive and documentary), and their secure transmission and maintenance" and once inactive, it must be protected "by physically transferring them to a neutral third party and implementing intellectual control through archival description" (Duranti; MacNeil, 1997, p. 57-62).

Theory was operationalized in a collaboration between the UBC research team and the U. S. Department of Defense Records Management Task Force that saw the hypotheses of the UBC project expressed as activity models and entity relationship diagrams, and then translated into mandatory functional requirements for records management application software (DOD 5015.2 STD) (Duranti; MacNeil; Underwood, 1996; Thibodeau; Prescott, 1996). The validity of traditional archival and diplomatic concepts was therefore tested and found to provide a "powerful and internally consistent methodology for preserving the integrity of electronic records" (Duranti; MacNeil, 1997, p. 64).

INTERPARES: INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS

The longest running, continuously funded research[5] into the preservation of authentic digital records has been the InterPARES Project at the University of British Columbia. InterPARES has developed knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form, and provided the basis for standards, policies, strategies and plans of action capable of ensuring the longevity of such material and the ability of its users to trust its authenticity. International in scope, it is supported by an interdisciplinary process that has included a wide range of academic and professional fields, from sciences and the arts, to computer engineering and law (Duranti; MacNeil, 1997; Duranti, 2005; Duranti; Preston, 2008).

InterPARES has been carried out in three completed phases, and a fourth phase is in progress. The first phase, InterPARES I (1999-2001), sought to address the problem of assessing and maintaining authenticity of records (primarily born digital textual records in databases and document management systems) when they come into archival custody. InterPARES 1 was organized around four domains of inquiry for inactive electronic records, the first of which developed the conceptual requirements for preserving authentic electronic records and the identification of elements necessary to maintain their authenticity over time. The concepts of reliability, authenticity, record, and electronic record adopted and developed in the UBC Project formed the basis of inquiry. Research was conducted from the point of view of the preserver and the life-cycle model of administrative and legal records generated in databases and document management systems (Duranti, 2001; Duranti; Preston, 2005; Duranti, 2007).

The Authenticity Task Force explained the rationale for establishing conceptual requirements for assessing the authenticity of electronic records. It recognized that the records

5 InterPARES has been funded through all four phases by the Social Sciences and Humanities Research Council of Canada (SSHRC).

relied upon by their creator in the usual and ordinary course of business are presumed to be authentic. In the digital environment, however, records are at risk of intentional or unintentional alteration, which may be difficult to determine. The Task Force further distinguished electronic records that exist as created, and those that have undergone change of some kind (for example format change or migration). Both types are considered authentic if relied upon by their creator. The authenticity of electronic records is threatened whenever they are transmitted across space or time, necessitating the means for assessing and maintaining authenticity to support the presumption that records continue to be as claimed and free from corruption or undocumented modification (MacNeil; Gilliland-Swetland, 2005, p. 22, 49).

Conceptual findings of the Task Force provided requirements for authenticity, defined the concept of authentication, and introduced the concept of the presumption of authenticity. The Task Force found that, to assess the authenticity of an electronic record, the preserver must be able to establish its identity and demonstrate its integrity. The identity of a record refers to the attributes that uniquely characterize it and distinguish it from other records, while the integrity of a record refers to its wholeness and soundness, that is, to the fact that it is complete and uncorrupted in all essential respects. An important finding of the research was that "complete and uncorrupted in all essential respects" does not necessarily require the record to maintain the same bit structure, but means that the message the record is meant to communicate in order to achieve its purpose is unchanged. The preserver must assess the authenticity of records transferred from their creator. Thus a presumption of authenticity is an inference based on evidence about how the records have been created and maintained. Evidence may come from the creator, or through further analysis to verify authenticity, such as comparison of the records with copies preserved elsewhere (redundancy), forensic analysis, testimony of a third party, or analysis of audit trails (MacNeil; Gilliland-Swetland, 2005, p. 47-51).

The Task Force developed benchmark requirements, that give reasonable assurance of authenticity prior to transfer of records from their creator to the trusted preserver (trusted recordkeeping), and baseline requirements that support the production of authentic copies of electronic records that have been transferred to the preserver (trusted custodianship). The benchmark requirements included:

- identification of fundamental information that establishes a record's identity and allows for demonstration of its integrity, explicitly expressed and inextricably linked to the record (may appear on face of record or in metadata);
- evidence of access privileges that show the assignment of authority and capacity to carry out administrative action accompanied by exclusive technical capability to exercise such responsibility;
- establishment and implementation of procedures to prevent, discover, and correct loss or corruption of records (regular backups of both files and systems);
- establishment and implementation of procedures to guarantee the continuing identity and integrity against media deterioration and across technological change;

- establishment and control of documentary forms (down to the level of record elements) associated with procedures either according to juridical requirements or institutional policy.

The creator must also specify details governing authentication of records, establish procedures to identify the official record from among multiple copies, and establish and implement procedures to determine what documentation must be removed and transferred to preservation with the record (i.e. what information is required to establish and maintain identity and integrity).

The baseline requirements to support the production of authentic copies require that:

- procedures and systems used to transfer, maintain and reproduce embody adequate and effective controls to guarantee integrity and identity, including unbroken chain of custody; security and control procedures implemented and monitored; content unchanged after reproduction;
- activity of reproduction must be documented, including date of reproduction and name of responsible person; relationship between records acquired from creator and copies produced by archivists; impact of reproduction process on form, content, accessibility and use; details of any elements not fully and faithfully reproduced;
- description of all technological changes are included as part of archival description (a collective attestation of authenticity of records in the archival group and all their interrelationships) (MacNeil; Gilliland-Swetland, 2005, p. 204-219).

The Task Force found several deficiencies in the electronic systems they observed with respect to creating, maintaining and preserving records, as defined by archival diplomatics. For example, electronic systems are often designed to manage data rather than records – that is, fixity requirements for records do not exist. Identity information is often implicit in the records, with the consequence that key indicators of identity may be lost when the records are transferred out of the record creating or record keeping system. Indifference of records creators to issues of authenticity were also common, replaced by confidence in the technology to protect the authenticity of the records (MacNeil; Gilliland-Swetland, 2005, p. 52).

The Task Force also discussed limitations of diplomatics as an analytical tool – a discussion that paved the way to the second phase of the InterPARES (MacNeil, 2004). InterPARES 2 (2002-2007) returned to the perspective of the records creator. In addition to dealing with issues of authenticity, it researched issues of reliability and accuracy during the entire lifecycle of records, from creation to permanent preservation. The project was organized in three research domains: digital records creation and maintenance; authenticity, reliability, and accuracy of digital records in the artistic, scientific, and governmental sectors; and methods of appraisal and preservation. These domains were supported by four cross-domains that modeled the records life cycle and continuum (developing the Chain of Preservation model and the Business-Driven Recordkeeping Model), investigated the role of metadata (description cross-domain), structured the relationship between creators and preservers through policy (policy cross-domain) and studied the terminology that underpinned relevant issues across

disciplines (terminology cross-domain). The focus of research was on records produced in complex (dynamic and interactive) digital environments in the course of artistic, scientific and governmental activities (Duranti; Preston, 2008).

The Domain 2 Task Force, investigating authenticity, reliability and accuracy of digital records, carried out case studies in the artistic, scientific, and governmental sectors. Building on the work of InterPARES I, the Task Force was immediately confronted with the challenges of diverse domain understanding of what is meant by the terms 'record' and 'authenticity' in the three areas of investigation, and the fact that the structure and function of digital entities created in art and science often did not resemble those in legal or administrative contexts. It was cognizant of the fact that the diversity encountered in the case studies also reflected lines of thought about the constructed nature of authenticity developing in the postmodern archival literature. It found that, while the benchmark requirements were useful for measuring a presumption of authenticity, they could be difficult to apply or adapt depending on the nature of the creator's records, and in some cases were not sufficient to preserve the kinds of authenticity valued by the creator. It also found in several disciplines limited definitions of authenticity that related it most closely to integrity. Frequently authenticity was presumed from the circumstances of record creation, or linked to technological methods of authentication. Within the sciences, for example, the term 'authenticity' is rarely used, although information about identity, captured in metadata, integrity, ensured through authentication and security measures, and provenance, or lineage, is crucial (Roeder et al., 2008, p. 141-163).

Scientific disciplines do not normally use the word 'authenticity' when describing datasets, although the fundamental archival concepts are often addressed, either implicitly (trusted source) or explicitly (data lineage, integrity). They are more concerned with issues of completeness, reliability, accuracy, and integrity. Many have issues of legacy datasets that have been digitized. In these situations, if the source of the original data can be assumed trustworthy, then the data acquired are presumed reliable and accurate (Hackett; Underwood; Eppard, 2005, p. 33-41). In the field of Geography and Geomatics, authenticity is assessed through analysis of data lineage, which is one of at least seven elements comprising 'spatial data quality'. Data lineage information records the chain of transmission of a dataset from the moment of data collection. It is the history of a dataset from collection through stages of compilations, corrections, conversions, transformations ((Hackett; Underwood; Eppard, 2005, p. 31-32). In scientific fields generally, accuracy of data receives the most attention, with primacy given to data quality, which includes the concept of authenticity, (normally articulated as data provenance or lineage) (Roeder et al., 2008, p. 133-137). Metadata are means of attesting to and assessing a dataset's authenticity – authenticity is linked to a clear lineage recorded in the accumulating metadata surrounding the data.

The preservation of authentic datasets of information collected through observation, computation, or experiment is of increasing concern (National Science Foundation, 2005, apud Lauriault et al., 2007, p. 132, n. 32). These data may be historical recordings of natural events that can never be replicated or recollected, may concern models for complex com-

putations, such as climate change models, or be experimental, reproduceable only at prohibitive cost, or not at all. Scientists give primacy to data quality, which they equate with authenticity, and base on provenance or lineage, and traceability, expressed through metadata or data-quality parameters. As stated previously, the term "authenticity" is not often used, despite the discussion of qualities of identity and integrity through concepts of data provenance and data lineage. Lineage is represented in an audit trail that provides the data with assurances about its source or pedigree, and fitness for use (Lauriault et al., 2007, p. 153).

The trustworthiness of official statistics relies on citizen confidence that they are independently produced and free from bias or political interference. Statistics are based on data collected through a variety of government and research agencies. Increasingly, governments are making large datasets available for public scrutiny and analysis through official programs of open data. A comparison of open data policies in national and regional jurisdictions across North America (US and Canada) enacted from 2009 through 2014 show, however, that specific quality controls are generally lacking. For example, open data policy recommendations such as publishing metadata, making available information about the data creation process, sharing of code or publishing open source, and requiring the use of unique identifies – all critical mechanisms for establishing authenticity, provenance and data quality – are addressed in a very few, if any, jurisdictions (Sunlight Foundation 2014a; Sunlight Foundation 2014b).

In government, concepts of authenticity, accuracy and reliability are seldom addressed directly. Concerns about authenticity in the electronic environment tend to be generic, and difficult to address because of imprecise terminology, which as used in the governmental sector in discussing digital records is at times vague or inconsistent. This is particularly true for words like "authenticity," "accuracy" and "reliability," which are not technical terms in general parlance, but words with common sense, everyday meanings. The research team found that the concept of authenticity was frequently equated with integrity. The conclusion for the government sector was that, although concern for authenticity of records was high, the use of terminology was loose. Authenticity was often presumed rather than assessed, particularly in instances where authentication techniques are employed (Roeder et al., 2008, p. 126-133).

Metadata are the machine- and human-readable assertions about information resources that allow for physical, intellectual and technical control over those resources. Users create and attach, and then maintain and preserve metadata, either automatically and/or manually, when maintaining their digital records, documents, and data. These metadata may be technical, administrative, or descriptive. They codify and track the identity and integrity of the material over time and across technological change. The Description Cross-Domain Task Force examined the crucial role of recordkeeping metadata in the creation of authentic records and the maintenance of their authenticity over time and across technological change. Their premise was that detailed and trustworthy metadata were key to the creation of reliable and preservation of authentic digital records (Gilliland, 2008; Gilliland; McKemmish, 2012). The importance of recordkeeping metadata has been acknowledged

since the 1990s (e.g. Hurley, 1995), but in practice, metadata frequently still remain underused and misunderstood (Isaza, 2010).

InterPARES 3 (2007-2012) built upon the findings of InterPARES 1 and 2, as well as other digital preservation projects worldwide, to put theory into practice, applying the results of the previous two phases through case studies with small and medium-sized organizations, or those with limited resources, and general studies. One general study built on the work of the Description Cross-Domain of InterPARES II and attempted to develop an application profile for authenticity metadata based on the benchmark and baseline requirements as articulated in the Chain of Preservation model (Tennis; Rogers, 2012a, 2012b). This work is ongoing.

AUTHENTICITY IN RELATED DIGITAL PRESERVATION RESEARCH PROJECTS

Because of the cross-disciplinary nature, sweeping scope, and staggering cost of digital preservation, research is often carried out by national and international alliances of universities, libraries and archives, government agencies, business and industry. Each alliance is defined by its particular epistemic perspective and purpose. However, cooperation and collaboration, if not always agreement, are constants across the entire research community. There are also major national initiatives undertaken by national archives and/or libraries, such as those in Australia, the United States, and Denmark.

Meaningful engagement with digital information resources requires predictability and comprehensiveness, interoperability, transactionability, and preservability. Digital preservation is partly a technical problem, but more importantly, it is "one component of a broad aggregation of interconnected services, policies, and stakeholders which together constitute a digital environment" (Lavoie; Dempsey, 2004). Preservation research can be classified according to its particular focus: the development of standards, frameworks, and repository systems (e.g. Oais); defining and using/sharing metadata schemas (e.g. Premis, OAI); the nature of digital objects (e.g. InterPARES, InSPECT); technologies of preservation (e.g. preservation-aware storage); and file formats and object identification (e.g. JSTOR, JHOVE). All of these projects share a common goal, that of preserving digital objects that can be trusted, although not all of them approach authenticity explicitly. Of note are Oais and Caspar, both of which are connected in different ways to InterPARES. A comprehensive summary of preservation research from the early 1990s through the 2000s is found in Anne Gilliland's book, *Conceptualizing 21st-Century Archives* (2014).

The Open Archival Information System (Oais) Reference Model is a high-level model and the benchmark for digital preservation systems, addressing all aspects of long-term preservation of digital information: ingest, archival storage, data management, access, dissemination, and migration to new media and forms. Developed in 2002 by the Consultative Committee for Space Data Systems, the Oais is now an approved ISO standard (ISO 14721:2003) and has undergone several revisions, the most recent in 2012 (CCSDS 2012). This latest revision addresses authenticity requirements more directly than previous revisions; however, as it is a high level standard, it does not dictate how authenticity is to be ensured or protected.

It defines authenticity as "the degree to which a person (or system) regards an object as what it is purported to be. Authenticity is judged on the basis of evidence" (Giaretta et al., 2009, p. 69). Part of the necessary evidence is provided by Provenance Information, which tells the origin of the source of the Content Information, documents changes to it and the chain of custody since creation. Authenticity, a stated objective of long-term preservation, is deemed the responsibility of the repository to protect (CCSDS, 2012, 1.9–1.14). When digital resources considered for preservation include natural science and social science datasets, government, health, and economic data submitted to national data archives conforming to the Oais standard, the focus of authenticity requirements shifts from the record or digital object in general to the authenticity needs of a specific community of users.

Caspar (Cultural, Artistic, and Scientific Knowledge for Preservation, Access, and Retrieval) developed an Authenticity Conceptual Model that is Oais-compliant, technology-neutral, and domain-independent (Lamb, 2009). The model consists of an Authenticity Protocol, applied to an Object Type, and comprising Authenticity Steps (Reference, Provenance, Fixity, Context, Access/Rights) (Guercio, 2008; Guercio; Michetti 2009a; Giaretta, 2011, p. 209-210). Authenticity Protocols (APs) are defined as "procedures to be followed in order to assess the authenticity of specific type of Digital Resource (DR)". Caspar conducted its research based on certain assumptions about digital preservation: that it is not enough to preserve just the bits, but also information and knowledge; that preservation is a process of transforming and enriching content through different technological strategies to adapt it to new constraints of rendition and playability, to preserve its intelligibility and (re)usability, and to ensure its integrity and authenticity (Guercio, 2008; Guercio; Michetti, 2009a; Guercio; Michetti, 2009b; Salza et al., 2012).

Built on the foundations of Caspar, Aparsen (Alliance for Permanent Access to the Records of Science in Europe Network), launched in 2010, aims to bring together work in digital preservation carried out across Europe. Aparsen (2012) defines success as establishing "coherence and general direction of travel of research in digital preservation, with an agreed way of evaluating it and the existence of an internationally recognized Virtual Centre of Excellence". Early in 2012 Aparsen released a report on the implementation and testing of domain-specific authenticity protocols. This comprehensive report begins with a "State-of-the-Art" outline of related projects in digital preservation research – first on the list is InterPARES, followed by Caspar. These three projects are highly connected in purpose and complementary in approach. Aparsen adopts the Caspar definition of authenticity, which is general and high level, and the theoretical underpinnings of InterPARES, and has formalized an authenticity management model, based on the principle of performing controls and collecting authenticity evidence in connection to specific events of the digital object's lifecycle. This allows the assessor – preserver or user – to trace back all the transformations the digital object has undergone since its creation and that may have affected its authenticity (Salza et al., 2012, p. 8).

EXPLORING NEW MODELS OF RECORD AND RECORD AUTHENTICITY

In the late 2000s and into the 2010s, the continuing advance of digital technology further complicated recordkeeping and archival practice. The failure of record trustworthiness in the digital environment has been attributed as a significant factor in national banks crises (cf. Lemieux, 2001), and in the global financial crisis (cf. Tonkiss, 2009; Gurría, 2009; Lemieux; Limonad, 2011). Authenticity remains a critical issue in research into digital preservation and access, with a number of major projects funded by the European Union through their EU Framework Programme (cf. Giaretta, 2011; Strodl; Petrov; Rauber, 2011). Issues of trust and confidence in the Web are also the subject of computer science research (Cofta, 2007; Cofta, 2013).

Through the 2000s the concept of record was revisited (cf. Lemieux, 2001; Yeo, 2007; Yeo, 2008), and with it, the interrelated concepts of authenticity and trust (cf. Yeo, 2013). The literature spans not only the technological developments that have brought so much change to records professions and records-related issues, but significant developments in archival worldview. This is reflected most clearly in the theoretical archival literature, where the rise of critical, hermeneutic, or pragmatic epistemologies (Hjørland, 2008) resulted in new interpretivist concepts of archival functions (Cook, 2001; Nesmith, 2002; Cook, 2013), and of custodianship (the continuum model) (Upward, 1996; Upward, 1997; McKemmish, 2001; Upward, 2005). Different articulations of the concept of 'record' continue to emerge, arising from the particular challenges of increasingly complex digital technological infrastructures (Duranti, 2009; Duranti; Endicott-Popovsky, 2010; Lemieux; Limonad, 2011; Thibodeau, 2013; Lemieux, 2014).

As well, archival scholars are exploring the application of domain-specific meanings of authenticity to archival practice (cf. Lauriault et al., 2007; MacNeil; Mak, 2007; Duncan, 2009; Mak, 2012). At the root of these explorations is the idea that authenticity is a social construction dependent on the context or discipline within which it is defined, interpreted, and required. If one subscribes to the view that digital resources are "in a continuous state of becoming" as they are created, used, migrated, preserved, and accessed over time, then so too is the nature of their authenticity (MacNeil; Mak, 2007, p. 26).

THE ROLE DIGITAL FORENSICS AND INFORMATION ASSURANCE

Archivists have begun to create research alliances with digital forensics practitioners in order to develop and extend the applicability of diplomatics in the field of digital preservation with a focus on authenticity, reliability, and accuracy (Duranti, 2009; Kirschenbaum; Ovenden; Redwine, 2010; John, 2012; Rogers; John, 2013). Digital forensics offers archivists another way of conceptualizing digital objects and assessing their integrity and authenticity that can complement and be complemented by existing archival methodologies (Duranti; Endicott-Popovsky, 2010; Duranti; Rogers, 2011). Archival repositories are motivated to adopt digital forensics tools to help support description and context, integrity, version detection, and identification and protection of authenticity (John, 2012, p. 11).

Two fundamental problems that digital forensics – and digital archives – must deal with are complexity and quantity. These derive from the nature of digital technology, and therefore are common to all information domains that deal with digital material. All digital objects at the lowest level of their existence are streams of bits – series of 0s and 1s. These are not understandable by humans without the intervention of layers of technology through which the data are translated (Carrier, 2003). Part of determining authenticity depends on assurance of integrity of each layer of abstraction. Digital forensics offers archival science a more granular and nuanced understanding of integrity. While archivists have defined integrity simply as the quality of being complete and unaltered in all essential respects, focusing on the logical manifestation of the record, digital forensic scientists distinguish several levels of integrity at both the physical and the logical level – at the level of the bit stream, the data, the computer, or the system. However, not all layers need to be or can be maintained without change throughout the life of the object. Analyzing the object through abstraction layers offers the possibility of a more nuanced view of authenticity.

The second problem is that of quantity. Faced with terabytes or more of data, digital forensics specialists, archivists, scientists, and trusted recordkeepers in all domains need to be able to group data by layers, type, or other means in order to analyze them and assess their authenticity. This has been referred to variously as "information inflation" (Paul; Baron, 2007), or the "digital tsunami" (Lemieux; Baron, 2011).

Digital forensics also sits at the core of the information assurance and security (IAS), of which authenticity is an important component. The National Institute of Standards and Technology (NIST) defines information security as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability", and information assurance as "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (National Institute of Standards and Technology, 2013). IAS has been described as a multidisciplinary knowledge domain (Cherdantseva; Hilton, 2013), and a business-wide issue that extends far beyond the IT department (ICA, 2013). However, authenticity has not always been included explicitly in computer security models. The first and best known conceptual computer security model is the CIA-triad (confidentiality, integrity, and availability). Since its introduction in the mid-1980s security experts have challenged the adequacy of the model and proposed extensions (Cherdantseva; Hilton, 2013). The Parker hexad adds utility, authenticity, and possession, proposing that integrity, the characteristic of being complete and whole and free from corruption or manipulation, was insufficient without the assurance also of authenticity, or "conformance with reality" (Parker, 1998; Kabay, 2013). Most recently, Cherdantseva and Hilton (2013) have proposed a reference model they call the IAS Octave: confidentiality, integrity, availability, privacy, authenticity and trustworthiness, non-repudiation, accountability, auditability.

While most of the digital forensics literature focuses on practical and technical aspects of practice, there are articles spanning the last fifteen years by both practitioners and scholars that are conspicuous for their explicit acknowledgement of parallels between the disciplines of digital forensics and archival/records/information management (cf. Rowlingson, 2004; Irons, 2006; Ferguson-Boucher; Endicott-Popovsky, 2008; Lemieux; Baron, 2011). These authors touch variously on issues of appraisal, records management, and the application of principles of diplomatics, and suggest fertile ground for further research. They are, as yet, the exception – lone voices from the digital forensics and legal perspective embracing archival and records management principles. Clearly, however, this is beginning to change, inspired by projects such as the Digital Records Forensics Project, Records in the Cloud, and InterPARES Trust at the University of British Columbia, and collaboration between the School of Library, Archival and Information Studies at UBC and the Center for Information Assurance and Cybersecurity at the University of Washington (Duranti; Endicott-Popovsky, 2010; Duranti; Rogers, 2011).

STUDIES OF PRACTITIONER BEHAVIOR AND AUTHENTIC RECORDS

Few studies have been conducted on the behavior of records professionals in ensuring, maintaining, and assessing record authenticity. An exploratory pilot study on practitioners' concepts of authenticity in their work activity was conducted in 1998. Park noted that while questions about authenticity of electronic records had been the subject of archival and preservation research, a systematic investigation of practitioner behavior had not been undertaken. She asked: What does the concept of authenticity mean to practitioners? How do practitioners define the concept of authenticity? And, is the concept of authenticity understood differently in different professional domains? Among her results, she found that while practitioners were highly aware of the concept of authenticity in both paper and electronic records, less than half have been required to authenticate records. Park compared treatment of paper records with treatment of electronic records, and used content analysis to study the use of terminology. She found that practitioners did not perceive a difference between paper and electronic records with respect to authenticity, although they recognized that the means of authenticating records will be different (Park, 2001). She concluded that research and practice were far apart, and work was needed to bridge the gap.

The relationship between ICTs, authentic records, and accountability was examined in an empirical study of accountability forums and public administrations (Meijer, 2003). Meijer found that authenticity of records is protected by a combination of technological, organizational (division of tasks), and institutional (norms, values, cognitive scripts) safeguards. Accountability for a, for example international courts, need authentic digital records to reconstruct actions and decisions of government officials and organizations and are willing to rely on perceived or stated safeguards, and only question the authenticity of records if they are confronted with clear evidence of tampering.

FINAL REMARKS

The literature shows that awareness of the value of confidence in record authenticity has been a common thread, if not an explicit objective, of research into the nature and preservation of digital records. Evaluating authenticity lends a measure of confidence, stability, and fixed reference points – that is, evidence of trustworthiness (MacNeil, 2001, p. 42). An assessment of authenticity relies on both structural assurances and situational normality (McKnight; Chervany, 2001, p. 37-38). Several streams of current research are actively pursuing models of authenticity measures (Salza et al., 2012; Guercio; Salza, 2013), secure provenance (Hasan; Sion; Winslett, 2007; Lu et al., 2010), and preservation-aware storage (Factor et al., 2009). The fourth phase of InterPARES is researching issues of trust, in which authenticity is an important part, in records online. Records created, managed and preserved in online – cloud – environments are subject to all the challenges and risks identified through research conducted throughout the 1990s and 2000s. In addition, they face new challenges arising from the global nature of the internet. Identifying provenance, authorship, and responsibility for ownership and control, and jurisdictional authority all increase the risks to our digital heritage.

While much current research focuses on digital preservation and legal issues such as privacy, security, and access, what has been lacking is a measure of how records professionals are handling authenticity of digital records on a day-to-day basis. Park's work of more than a decade ago demonstrated that research and practice were far apart, and the continued research focus on and concern about digital records' authenticity would suggest that this has not changed. Little has been done since these Park's work to map the knowledge gained through research to the practice of records professionals, until now. My premise that, despite strides in knowledge and awareness of digital records issues among records professionals, and complex research into authenticity models as part of preservation research, the gap between research and practice still exists and may be widening was supported by my research (Rogers, 2015). This literature review laid the groundwork for that study.

Bibliographical references

ALLIANCE FOR PERMANENT ACCESS (Aparsen). *About APARSEN*. [S.l.], 2012. Available in: <www.alliancepermanentaccess.org/>.

BEARMAN, David. The Implications of Armstrong v. Executive of the President for the Archival Management of Electronic Records. *American Archivist*, USA, n. 56, p. 674-90, (Fall) 2014.

BEARMAN, David; TRANT, Jennifer. Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process. *D-Lib Magazine*, Virginia, n. June 1998. Available in: <http://www.dlib.org/dlib/june98/06bearman.html>.

CARRIER, Brian. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence*, USA, 1 (4), p. 1-12, 2003.

CHERDANTSEVA, Yulia; HILTON, Jeremy. A Reference Model of Information Assurance & Security. In: *Institute of Electrical and Electronics Engineers (IEEE)*. p. 546-55. Doi:10.1109/ARES.2013.72.

COFTA, Piotr. *Trust, Complexity and Control*: Confidence in a Convergent World. 1st New Jersey, ed. Wiley. Set 2007. 310 p.

_____. *The Foundations of a Trustworthy Web*. Boston, Delft: Now Publishers, 2013. Avaliable in: <http://dx.doi.org/10.1561/9781601986634>.

COMMITTEE ON ELECTRONIC RECORDS. *Guide for Managing Electronic Records from an Archival Perspective*. Paris: International Council on Archives, 1997.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS) (USA). *Reference Model for an Open Archival Information System (Oais)*: Recommended Practice Issue 2. [S.l.], 2012. Available in: <http://public.ccsds.org/publications/archive/650x0m2.pdf>.

COOK, Michael. *The Management of Information from Archives*. Aldershot, Hants, England ; Brookfield, Vt., U.S.A: Gower, 1986.

COOK, Terry. What's Past Is Prologue: A History of Archival Ideas since 1898 and the Future Paradigm Shift. *Archivaria*, Ontario, n. 43, p. 17-63, 1997.

_____. Archival Science and Postmodernism: New Formulations for Old Concepts. *Archival Science*, [S.l.], n. 1, p. 3-24, 2001.

_____. Evidence, Memory, Identity, and Community: Four Shifting Archival Paradigms. *Archival Science*, [S.l.], 13 (2-3), p. 95-120, 2013. Doi:10.1007/s10502-012-9180-7.

COUNCIL ON LIBRARY AND INFORMATION RESOURCES (Clir). *Authenticity in a Digital Environment*. Washington (D.C.), 2000. Available in: <http://www.clir.org/pubs/reports/pub92/pub92.pdf>.

DOLLAR, Charles. Appraising Machine-Readable Records. *The American Archivist*, Chicago, 41 (4), p. 423-30, 1978.

_____. Archivists and Records Managers in the Information Age. *Archivaria*, Ontario, n. 36, p. 37-52, (Autumn) 1993.

DUFF, Wendy M. Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC. *Archivaria*, Ontario, n. 42, p. 28-45, (Fall) 1996.

DUNCAN, Chris. Authenticity or Bust. *Archivaria*, Ontario, n. 68, p. 97-118, (Fall) 2009.

DURANTI, Luciana. Diplomatics: New Uses for an Old Science (Part I). *Archivaria*, Ontario, n. 28, p. 7-27, (Summer) 1989a.

_____. Diplomatics: New Uses for an Old Science (Part II). *Archivaria*, Ontario, n. 29, p. 4-17, (Winter) 1989b.

_____. Diplomatics: New Uses for an Old Science (Part III). *Archivaria*, Ontario, n. 30, p. 4-20, (Summer) 1990a.

_____. Diplomatics: New Uses for an Old Science (Part IV). *Archivaria*, Ontario, n. 31, p. 10-25, (Winter) 1990b .

_____. Diplomatics: New Uses for an Old Science (Part V). *Archivaria*, Ontario, n. 32, p. 6-24, (Summer) 1991a.

_____. Diplomatics: New Uses for an Old Science (Part VI). *Archivaria*, Ontario, n. 33, p. 6-24, (Winter) 1991b.

_____. Archival Science. In: *Encyclopedia of Library and Information Science*. New York, Basel, Hong Kong: Marcel Dekker, 59, p. 1-19, 1996a.

_____.The Thinking on Appraisal of Electronic Records: Its Evolution, Focuses, and Future Directions. *Archivi and Computer*, Italy, n. 6, p. 493-518, 1996b.

_____.The Archival Bond. *Archives and Museum Informatics*, [S.l.], 11 (3-4), p. 213-18, 1997.

_____. *Diplomatics*: New Uses for an Old Science. Lanham: Scarecrow Press, 1998a.

_____.The Odyssey of Records Management, Part 1. *Records Management Quarterly*, [S.l.], 23 (3), 1998b.

_____. The Odyssey of Records Management, Part 2. *Records Management Quarterly*, [S.l.], 23 (3), 1998c.

_____. The Impact of Digital Technology on Archival Science. *Archival Science*, [S.l.], 1 (1), p. 39-55, 2001. Doi:10.1007/BF02435638.

_____. Authenticity and Appraisal: Appraisal Theory Confronted With Electronic Records. In: INTERNACIONAL COLLOQUIUM ON LIBRARY AND INFORMATION SCIENCE: The Refined Art of Destruction: Records' Appraisal and Disposal, 3., 2002, Salamanca, Spain. *Proceedings*… Salamanca: University of Salamanca, 2002. Available in: <www.interpares.org/display_file.cfm?doc=ip1_dissemination_cpr_duranti_clis_2002.pdf>.

_____. The Long-Term Preservation of Accurate and Authentic Digital Data: The InterPARES Project. *Data Science Journal*, [S.l.], n. 4, p. 106-18, (October) 2005.

_____. Reflections on InterPARES: The InterPARES 2 Project (2002-2007): An Overview. *Archivaria*, Ontario, n. 64, p. 113-21, (Fall) 2007.

_____. From Digital Diplomatics to Digital Records Forensics. *Archivaria*, Ontario, n. 68, p. 39-66, (Fall) 2009.

DURANTI, Luciana; EASTWOOD, Terry. Protecting Electronic Evidence: A Progress Report on a Research Study and Its Methodology. *Archivi and Computer*, Roma, v. 3, p. 213-50, 1995.

_____ ; McNeil, Heather. Protecting Electronic Evidence: A Second Progress Report on a Research Study and Its Methodology. *Archivi and Computer*, Florida, VI (1), p. 37-70, 1996.

_____ et al. *Preservation of the Integrity of Electronic Records*. [S.l.]: Springer Science & Business Media, 2003.

_____; ENDICOTT-POPOVSKY, Barbara. Digital Records Forensics: A New Science and Academic Program for Forensic Readiness. *Journal of Digital Forensics, Security and Law*, Florida, 5 (2), p. 1-12, 2010.

_____; MACNEIL, Heather. The Preservation of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project. *Archivaria*, Ontario, n. 42, p. 46-67, (Spring) 1997.

_____; UNDERWOOD, William. Protecting Electronic Evidence: A Second Progress Report on a Research Study and Its Methodology. *Archivi and Computer*, VI (1), p. 37-70, 1996.

_____; PRESTON, Randy (eds.). *The Long-Term Preservation of Authentic Electronic Records*: Findings of the InterPARES Project. San Miniato (Italy): Archilab, 2005.

_____. *Research on Permanent Authentic Records in Electronic Systems (InterPARES), 2., Experiential. Interactive and Dynamic Records*. Padova: Associazione Nazionale Archivistica Italiana, 2008.

_____; ROGERS, Corinne. Educating for Trust. *Archival Science*, [S.l.], 11 (3-4), p. 373-90, 2011. Doi:10.1007/s10502-011-9152-3.

DURANTI, Luciana; THIBODEAU, Kenneth. The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES. *Archival Science*, [S.l.], 6 (1), p. 13-68, 2006.

EASTWOOD, Terry. What Is Archival Theory and Why Is It Important? *Archivaria*, Ontario, n. 37, p. 122-30, (Spring) 1994.

ERLANDSSON, Alf. *Electronic Records Management*: A Literature Review. Paris: International Council on Archives, 1997.

FACTOR, Michael et al. *Authenticity and Provenance in Long Term Digital Preservation*: Modeling and Implementation in Preservation Aware Storage. IBM Corporation, 2009. Available in: <http://www.research.ibm.com/haifa/projects/storage/datastores/papers/Auth_Prov_CamReady_sent.pdf>.

FERGUSON-BOUCHER; ENDICOTT-POPOVSKY, Barbara. Digital Forensics and Records Management: What We Can Learn from the Discipline of Archiving. In: CONFERECE: WHERE INFORMATION TECHNOLOGY, LAW AND RISK MANAGEMENT CONVERGE, 2008, Seattle. *Proceedings*: The Information Security and Compliance and Risk Management Institute. Seattle: University of Washington, 2008. p. 1-6.

GIARETTA, David. *Advanced Digital Preservation*. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011.

_____ et al. Significant Properties, Authenticity, Provenance, Representation Information and Oais. In: IPRES 2009: INTERNACIONAL CONFERENCE ON PRESERVATION OF DIGITAL OBECTS, 6., 2009, San Francisco: California Digital Library, p. 67-73. Available in: <http://escholarship.org/uc/cdl_ipres09>.

GILLILAND, Anne. Investigating the Roles and Requirements, Manifestations and Management of Metadata in the Creation of Reliable and Preservation of Authentic Digital Entities. In: DURANTI, Luciana; PRESTON, Randy. *Description Cross-Domain Task Force Report*. Internacional Research on Permanent Authentic Records in Electronic Systems, IP2, 2008. Vancouver, 2008. p. 305-59.

_____. *Conceptualizing 21st-Century Archives*. Chicago: Society of American Archivists, 2014.

_____; MCKEMMISH, Sue. Recordkeeping Metadata, the Archival Multivers, and Societal Grand Challenges. In: INTERNACIONALI CONFERENCE ON DUBLIN CORE AND METADATA APPLICATIONS, 2012, Kuching. *Proceedings*…, 2012. p. 106-13. Available in: <http://dcevents.dublincore.org/IntConf/dc-2012/paper/view/108/66>.

GRÄNSTRÖM, Claes. *Authenticity of Electronic Records*: A Report Prepared for Unesco. Paris: International Council on Archives (ICA), Commitee on Archival Legal Matters, 2002. Study 13-1.

GUERCIO, Maria. Authenticity and Oais: The Caspar Model and the InterPARES Principles & Outputs. In: DELOS SUMMER SCHOOL, 2008 June 11, Tirrenia. Available in: <http://www.interpares.org/display_file.cfm?doc=ip1-2_dissemination_ws_guercio_delos-ss_tirrenia_2008.pdf>.

_____; MICHETTI, Giovanni. *Modeling Authenticity, Part 1*. January, 2009a. Avaliable in: <http://www.alliancepermanentaccess.org/index.php/training/training-materials/lecture-3-modelling-authenticity-in-caspar/>.

_____. *Modeling Authenticity-Part 2*. September, 2009b. Available in: <http://www.alliancepermanentaccess.org/index.php/training/training-materials/lecture-3-modelling-authenticity-in-caspar/>.

_____; SALZA, Silvio. Managing Authenticity through the Digital Resource Lifecycle. In: AGOSTI, Maristella et al. (eds.). Digital Libraries and Archives. *Communications in Computer and Information Science*, Springer-Verlag Berlin Heidelberg, v. 354, p. 249-60, 2013. Available in: <http://link.springer.com/chapter/10.1007/978-3-642-35834-0_25>.

GURRÍA, Angel. *Responding to the Global Eceonomic Crisis*: OECD's Role in Promoting Open Markets and Job Creation. The Business and Industry Advisory Committee to the OECD. Lisboa,

2009. Available in: <http://www.oecd.org/fr/echanges/ndingtotheglobaleconomiccrisisoecdsroleinpromotingopenmarketsandjobcreation.htm>.

HACKETT, Yvette; UNDERWOOD, William; EPPARD, Philip. Part One – Case and General Studies in the Artistic, Scientific, and Governmental Sectors: Focus Task Force Report Yvette Hackett, Librar Y and Archives Canada William Underwood, Georgia Tech Research Institute Philip Eppard, University of Albany, State University of New York. In: DURANTI, Luciana; PRESTON, Randy (eds.). *Internacional Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2*: Experiential, Interactive and Dynamic Records, 2005. Available in: <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_1_focus_task_force.pdf>.

HASAN, Ragib; SION, Radu; WINSLETT, Marianne. Introducing Secure Provenanc. *Association for Computing Machinery (ACM) Press*, New York, n. 13, 2007. Doi:10.1145/1314313.1314318.

HJØRLAND, Birger; NICOLAISEN, Jeppe. *The Epistemological Lifeboat*, 2008. Available in: <http://www.iva.dk/jni/lifeboat/info.asp?subjectid=92>.

HURLEY, Chris. Ambient Functions: Abandoned Children to Zoos. *Archivaria*, Ontario, n. 40, (Fall) 1995.

INTERNACIONAL COUNCIL ON ARCHIVES (ICA). Committee on Archival Legal Matters. *Authenticity of Electronic Records*: A Report Prepared for Unesco. Study 13-1. Paris, France: International Council on Archives, 2002.

_____. ICC Belgium. *Belgian Cyber Security Guide*: Protect Your Information. FEB, EY, Microsoft, L-Sec, B-CCentre, Isaca. 2013. Available in: <http://www.iccbelgium.be/index.php/activities/becybersecure>.

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 15489-1:2001 Information and Documentation – Records Management, Part 1: General*, 2001. Available in: <http://www.iso.org/iso/iso_catalogue.htm>.

INTERPARES. *InterPARES 3 Project: Glossary*, 2012. Available in: <http://www.interpares.org/ip3/ip3_terminology_db.cfm?letter=p&term=38>.

INTERPARES Trust. *Www.interparestrust.org*. 2015. Available in: <www.interparestrust.org>.

IRONS, Alastair. Computer Forensics and Records Management: Compatible Disciplines. *Records Management Journal*, Macclesfield, 16 (2), p. 102–12, 2006. Doi:10.1108/09565690610677463.

ISAZA, John. *Metadata in Court*: What RIM, Legal and IT Need to Know. Pittsburgh, PA: ARMA International Education Foundation, 2010. Available in: <http://www.armaedfoundation.org/pdfs/Isaza_Metadata_Final.pdf>.

JENKINSON, Hilary. *A Manual of Archive Administration*. New and Revised. London: Percy Lund, Humphries & Co., 1937. Available in: <http://www.archive.org/details/manualofarchivea00iljenk>.

JOHN, Jeremy Leighton. *Digital Forensics and Preservation.* Great Britain: Digital Preservation Coalition and Jeremy Leighton John: Charles Beagrie Ltd., 2012. Available in: <http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf>.

KABAY, M. E. PHD, CISP-ISSMP. PPT course notes. *The Parkerian Hexad*. Northfield, 2013. Available in: Available in: <http://www.mekabay.com/overviews>.

KIRSCHENBAUM, Matthew G. et al. *Digital Forensics in Born Digital Cultural Heritage Collections*. Washington, D.C.: Council on Library and Information Resources, 2010.

LAMB, David. *CASPAR*. Edinburgh: Digital Curation Centre, 2009. Available in: <http://www.dcc.ac.uk/resources/briefing-papers/technology-watch-papers/caspar>.

LAURIAULT, Tracey P. et al. Today's Data Are Part of Tomorrow's Research: Archival Issues in the Sciences. *Archivaria*, Ontario, n. 64, p. 123-80, (Fall) 2007.

LAVOIE, Brian; DEMPSEY, Lorcan. Thirteen Ways of Looking at... Digital Preservation. *D-Lib Magazine*, Virginia, 10 (7/8), 2004. Doi:10.1045/july2004-lavoie.

LEMIEUX, V. Let the Ghosts Speak: An Empirical Exploration of the Nature of the Record. *Archivaria*, Ontario, n. 51, p. 81-111, 2001.

_____. Toward a 'Third Order' Archival Interface: Research Notes on Some Theoretical and Practical Implications of Visual Explorations in the Canadian Context of Financial Electronic Records. *Archivaria*, Ontario, 78 (0), 2014. Available in: <http://journals.sfu.ca/archivar/index.php/archivaria/article/view/13493>.

_____; BARON, Jason R. Overcoming the Digital Tsunami in E-Discovery: Is Visual Analysis the Answer? *Canadian Journal of Law and Technology*, Nova Scotia, 9 (33), p. 1-15, 2011.

_____; LIMONAD, L. What 'Good' Looks Like: Understanding Records Ontologically in the Context of the Global Financial Crisis. *Journal of Information Science*, Thousand Oaks, 37 (1), p. 29-39, 2011. Doi:10.1177/0165551510391359.

LU, Rongxing et al. Secure Data Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing. In: ACM SYMPOSIUM ON INFORMATION, COMPUTER AND COMMUNICATIONS SECURITY, 5., 2010, Beijing. *Proceedings…* Beijing: ACM Digital Library, Association for Computing Machinery, 2010. Available in: <http://dl.acm.org/citation.cfm?id=1755688>.

LYNCH, Clifford. Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust. In: *Authenticity in a Digital Environment*. Washington, D.C.: Council on Library and Information Resources, 2000. Available in: <http://www.clir.org/pubs/reports/pub92/lynch.html>.

MACNEIL, Heather. *Trusting Records*: Legal, Historical, and Diplomatic Perspectives. Dordrecht: Kluwer Academic, 2000.

_____. Trusting Records in a Postmodern World. *Archivaria*, Ontario, n. 51, p. 36-47, (Spring) 2001.

_____. Contemporary Archival Diplomatics as a Method of Inquiry: Lessons Learned from two Research Projects. *Archival Science*, (S.l.), 4 (3-4), p. 199-232.

_____; GILLILAND-SWETLAND, Ann. Authenticity Task Force Report. In: DURANTI, Luciana (ed.). *The Long-Term Preservation of Authentic Electronic Records*: Finding of the InterPARES Project. San Miniato (Italy): Archilab, 2005.

_____; MAK, Bonnie. Constructions of Authenticity. *Library Trends*, Baltimore, 56 (1), p. 26-52, 2007.

MAK, Bonnie. On the Uses of Authenticity. *Archivaria*, Ontario, n. 73, p. 1-17, (Spring) 2012.

MCKEMMISH, Sue. Placing Records Continuum Theory and Practice. *Archival Science*, (S.l.), 1 (4), p. 333-59, 2001. Doi:10.1007/BF02438901.

MCKNIGHT, D. Harrison; CHERVANY, Norman. Trust and Distrust Definitions: One Bite at a Time. In: FALCONE, R. *Trust in Cyber-Societies*. Berling; Heidelberg: Springer-Verlag, 2001, p. 27-54.

MEIJER, Albert Jacob. Trust This Document! ICTs, Authentic Records and Accountability. *Archival Science*, (S.l.), 3 (3), p. 275-90, 2003. Available in: <doi:http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/s10502-004-1287-z>.

MILLAR, Laura. Authenticity of Electronic Records: A Report Prepared for Unesco and the International Council on Archives. Study 13-2. Paris: International Council on Archives, 2004. Avai-

lable in: www.ica.org/sites/default/files/ICA_study_13-2-Authenticity-of-eletronic-records-ICA-Report-to-UNESCO_EN.pdf.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Nara). The History of the Electronic Records and ERA. *National Archives*: Electronic Records Archives. College Park, 2015. Available in: <http://www.archives.gov/era/about/history.html>.

NATIONAL INSTITUTE OF STANDARDS AND TECNOLOGY. *Glossary of Key Information Security Terms*. NISTIR 7298 Revision 2. Gaithersburg, 2013. Available in: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.

NAUGLER, Harold. Focus: The Machine Readable Archives Divison of the Public Archives of Canada. *Archivaria*, Ontario, n. 6, p. 176-80, (Summer) 1978.

_____. *The Archival Appraisal of Machine-Readable Records*: A RAMP Study With Guidelines. PGI-84/WS/27. Paris: Unesco, 1984. Available in: <http://unesdoc.unesco.org/images/0006/000635/063501eo.pdf>.

NESMITH, Tom. Seeing Archives: Postmodernism and the Changing Intellectual Place of Archives. *American Archivist*, USA, 65 (1), p. 24-41, 2002.

OXFORD English Dictionary. Oxford: Oxford University Press, 2014. Available in: <http://www.oed.com.ezproxy.library.ubc.ca/view/Entry/13314>.

PARK, Eun. Understanding 'Authenticity' in Records and Information Management: Analyzing Practitioner Constructs. *American Archivist*, USA, 64 (2), p. 270-91, 2001.

PARKER, Donn B. A New Framework for Information Security. In: PARKER, Donn B. *Fighting Computer Crime*: A New Framework for Protecting Information. New York: John Wiley & Sons, 1998, chapter 10. Available in: <http://common.books24x7.com.ezproxy.library.ubc.ca/toc.aspx?bookid=4856>.

PAUL, George L.; BARON, Jason R. Information Inflation: Can the Legal System Adapt? *Richmond Journal of Law & Technology*, Richmond, XIII (3), p. 1-41, 2007.

PEARCE-MOSES, Richard. *A Glossary of Archival and Records Terminology*. Society of American Archivists, 2005. Available in: <http://www.archivists.org/glossary/>.

ROEDER, John et al. Authenticity, Reliability and Accuracy of Digital Records in the Artistic, Scientific and Governmental Sectors: Domain 2 Task Force Report. In: DURANTI, Luciana; PRESTON, Randy. *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2*: Experiential, Interactive and Dynamic Records. Padova: Associazione Nazionale Archivistica Italiana, 2008. Available in: <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_3_domain2_task_force.pdf>.

ROGERS, C. *Virtual Authenticity* : Authenticity of Digital Records from Theory to Practice. Electronic Theses and Dissertations, Vancouver: University of British Columbia, 2015. Available in: <http://dx.doi.org/10.14288/1.0166169>.

_____; J. L, JOHN. Shared Perspectives, Common Challenges: A History of Digital Forensics & Ancestral Computing for Digital Heritage. In: THE MEMORY OF THE WORLD IN THE DIGITAL AGE: DIGITIZATION AND PRESERVATION, 2013, Vancouver, BC: Unesco, p. 314-36. Available in: http://www.unesco.org/webworld/download/mow/mow_vancouver_proceedings_en.pdf.

ROWLINGSON, Robert. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, Trier, 2 (3), p. 1-28, 2004.

SALZA, Silvio et al. *Report on Authenticity and Plan for Interoperable Authenticity Evaluation System*. (S.l.), 2012. Available in: <http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D24_1-01-2_3.pdf>.

STRODL, Stephan PETROV; Petar; BAUER, Andreas. *Research on Digital Preservation Within Projects Co-Funded by the European Union in the ICT Programme*. SCAPE Project, 2011. Available in: <http://www.scape-project.eu/wp-content/uploads/2014/08/SCAPE_digpres_research_ict.pdf>.

SUNLIGHT FOUNDATION. *Open Data Policies at Work*: A Bird's Eye View of Open Data Policies. Washington, December 23, 2014a. Available in: <http://sunlightfoundation.com/>.

_____. *Open Data Policy Guidelines*. Washington, December 23, 2014b. Available in: <http://sunlightfoundation.com/opendataguidelines/>.

TENNIS, Joseph T.; ROGERS, Corinne. Authenticity Metadata and the IPAM: Progress toward the InterPARES Application Profile. In: INTERNATIONAL CONFERENCE ON DUBLIN CORE AND METADATA APPLICATIONS, 2012, Kuching. *Proceedings…* Kuching, Sarawak, Malaysia: DCMI, 2012a, p. 38-45. Available in: <http://dcevents.dublincore.org/index.php/IntConf/dc-2012/schedConf/presentations>.

_____. *General Study 15*: Metadata Application Profiles for Authenticity. British Columbia: University of British Columbia, 2012b.

THIBODEAU, Kenneth. Wrestling with Shape-Shifters: Perspectives on Preserving Memory in the Digital Age. In: THE MEMORY OF THE WORLD IN THE DIGITAL AGE: DIGITIZATION AND PRESERVATION. *Conference Proceedings* edited by Luciana Duranti and Elizabeth Shaffer. Vancouver: University of Toronto; Unesco, 2013. p. 15-23. Available in: <http://www.unesco.org/webworld/download/mow/mow_vancouver_proceedings_en.pdf>.

_____; PRESCOTT; Daryll. Reengineering Records Management: The U. S. Department of Defense, Records Management Task Force. *Archivi and Computer*, Roma, VI (1), p. 71-78, 1996.

TONKISS, Fran. Trust, Confidence and Economic Crisis. *Intereconomics*, Hamburg, 44 (4), p. 196-202, 2009. Doi:10.1007/s10272-009-0295-x.

UPWARD, Frank. Structuring the Records Continuum. Part One: Post-Custodial Principles and Properties. *Archives and Manuscripts*, Sidney, 24 (2), p. 268-85, 1996.

_____. Structuring the Records Continuum. Part Two: Structuration Theory and Recordkeeping. *Archives and Manuscripts*, Sidney, 25 (1), p. 10-33, 1997.

_____. The Records Continuum. In: MACKEMMISH, Sue. *Archives*: Recordkeeping in Society. Wagga Wagga , N. S. W.: Centre for Information Studies: Charled Sturt University, Topics in Australasian Library and Information Studies, n. 24, p. 197-222, 2005.

YEO, Geoffrey. Concepts of Record (1): Evidence, Information, and Persistent Representations. *American Archivist*, USA, 70 (2), p. 315-43, 2007.

_____. Concepts of Record (2): Prototypes and Boundary Objects. *American Archivist*, USA, 71 (1), p. 118-43, 2008.

_____. Trust and Context in Cyberspace. *Archives and Records*, Tauton, 34 (2), p. 214-34, 2013. Doi:10.1080/23257962.2013.825207.

Recebido em 25/5/2016
Aprovado em 25/7/2016