Preservation as a Service for Trust

An InterPARES Trust Specification for Preserving Authentic Records in the Cloud

Adam Jansen
University of British Columbia
470-1961 East Mall
Vancouver, BC Canada V6T 1Z1
adamj@mail.ubc.ca

ABSTRACT

Questions regarding trust and authenticity of records stored in the Cloud, as well as the custodial obligations and storage management provided by the service provider of Internet-based records have yet to be resolved; but the adoption of Cloud-based technologies is not waiting for legislation or standards to resolve these issues. Therefore, there is an existing need clearly articulated requirements that provide effective, tested methods for documenting and maintaining the authenticity of records that are removed from creator's systems and placed into the custody and control of Cloud Service Providers. To address this need, Preservation as a Service for Trust (PaaST), part of the InterPARES Trust research project, is modelling a suite of preservation services that detail specific actions and attributes that capture, create or document metadata and activities that provide supporting evidence of the authenticity of records entrusted to the Cloud Service Providers.

KEYWORDS

Trust; Cloud Computing; Privacy; Access; Digital Preservation; InterPARES; Records

ACM Reference format:

Preservation as a Service for Trust Proceedings Paper in word format. In *Proceedings of the 14th International Conference on Digital Preservation, September 2017, Kyoto, Japan (iPRES2017).* 7 pages.

DOI:

1 Introduction

A recent survey conducted by O'Reilly Media revealed that 94% of respondents anticipated migrating to cloud technologies within the next five years [1]. The rapid increase in bandwidth availability, combined with the density increase in hard disk storage following Kryder's Law [2], has presented new commercial opportunities to level economy-of-scale savings through co-tenancy leveraging of computing resources in centralized datacenter mega-warehouses. These Internet-based service models (collectively referred to as 'the Cloud'), offer organizations both large and small the potential for lower upfront costs, decreased in-house technical staffing, and easy pay-as-you-go growth on demand. Given these numerous financial incentives, large numbers of both public and private organizations have been embracing the advantages that Cloud Services Providers CSPs) offer in order to create, store and access vast amounts in highly centralized, and some would argue highly attractive to hackers, internet-based environment.

Among these organizations that are relying upon CSPs to store and maintain their records are in public institutions, such as banks, public utilities, health care providers, and government departments, that the public has vested with an immense amount of trust and responsibility to protect their personal and sensitive data (e.g. social security numbers, birth dates, etc.). As these public trust institutions adopt these Cloud base services and migrate their records from internally hosted and managed data centers to Cloud-base services, the implications that such a paradigm shift entails is not fully understood. Traditional Records Management questions -- where are the records being stored, how are they being managed, where are all the copies hard disk, tape or otherwise – often are not asked or do not have answers. The very definition of the Cloud allows for dynamic and elastic provisioning, allowing for the rapid relocation and allocation of resources from a datacenter in one location to another (potentially in another country [3].

This global system of interconnected presents the issue of records from one jurisdiction – and, therefore, a specific set of record-related laws and regulations – can rapidly, fluidly and without knowledge of the records owner, to move into a storage location that resides within another jurisdiction – and a potentially conflicting or less favorable set of records access/disclosure laws – such as [4]. The legal liability for any damages that occur as a result of any security breaches of the CSP is either unclear or, if the basic service level agreement of any major Cloud storage provide is any indication, the reasonability of the record provider. Additionally, the expected response from the CSP in the event of disclosure, subpoena and access rules, regulations, and law regarding these records stored in the Cloud are unknowns. From an evidential perspective, a major area of concern when utilizing CSPs to store records of important legal value is whether those records, once entrusted to a CSP, can be trusted after they leave control of the creating organization [5]. Should those records be needed again, will sufficient documentation exist to establish a detailed chain of custody of those records have been created and accessible to establish the authenticity of the record retrieved from the CSP – from the time they left the creator's control through all

the movement within the CSPs mega-infrastructure and who accessed what and when? Whose responsibility is it to create and produce such documentation? To address these concerns of authenticity and legal admissibility, records creators and CSPs must work together to create the appropriate procedures and mechanisms to ensure that as records are transferred and/or moved from one location to another that they remain, and can continue to be proven to be, authentic.

2 Authenticity of Digital Records in Cyberspace

Records are a specific sub-set of data that are defined as any "document made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference" [6]. A record is considered to be authentic when its identity can be established and its integrity can be demonstrated. The identity of the record is derived from those attributes that uniquely characterize that record and are used to help distinguish one record from others that participated in the same, or similar, activities. The integrity of a record refers to the completeness of the record, in that the record possesses all of the its necessary parts to convey the message for which it was created and its condition is unimpaired [7]. Authenticity of records, from an Archival Science perspective, encompasses the entire context in which the records were created, accessed, stored and managed, from the moment of their creation through their entire life and eventual disposition. This is important in that records, as byproducts of the activity they provide evidence of, are granted a special allowance under the hearsay rules [8] that allows them to be submitted as evidence of the activity that created them. Therefore, in order for a record to continue to serve as a faithful witness of the activity that created it, it must remain demonstrably authentic; that is, it must be what it purports to be, free from any manipulation, substitution or falsification.

The presumption of authenticity is afforded to records when they are created to serve administrative needs during the usual and ordinary course of business. This presumption is strongly influenced by the methods and means of its creation, handling and chain of custody. When a record is moved across space (e.g. sent from one storage location to another over a network) or through time (e.g. set aside for later retrieval), the message for which the record was created must not be substantially altered in the process. Retaining the authenticity of records past their creation necessitates that those records be created, managed and stored in accordance with regular, documented procedures that can be attested to through an unbroken chain of custody [9]. When the records have been removed from the original system of creation, or passed onto a third-party custodian, documenting and providing evidence of how these records were stored and transmitted across space and through time becomes increasingly important, as important evidential metadata that supports that records authenticity is often lost in such movement. The stronger and more documented the procedures used in the handling, transfer and storage of the records, the stronger the record's presumption of authenticity that can be afforded to that record [10]. On the other hand, when a record is transferred into the care of a third-party custodian without documenting the procedures used or chain of custody, it becomes difficult to create post-facto to provide sufficient evidence of the identity and integrity of that record to support its presumption of authenticity. Once a record's presumption of authenticity is lost, it is nearly impossible to reassert.

3 Trust and Digital Records in an Increasingly Networked Society

The InterPARES Trust (ITrust) research project, under Project Director Dr. Luciana Duranti of the University of British Columbia and funded by the Social Sciences and Humanities Research Council of Canada (SSHRC), is exploring the trustworthiness of digital records uploaded to the Cloud with the goal to:

> ...generate the theoretical and methodological frameworks that will support the development of integrated and consistent local, national and international networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet, to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory [11].

The ITrust research team represents public and private institutions and universities from around the world with subject matter expertise in archival science, records management, diplomatics, law, information technology, communication and media, e-commerce, health informatics, cybersecurity, information governance and assurance, digital forensics, computer engineering, and information policy. The project has been organized into four regional teams (North America, Latin America, Europe, Asia) and a Multinational Organization team that are each focusing on a specific area of research that leverages their collective areas of expertise and geo-political environment. Represented amongst the larger institutions participating in the ITrust research project are: British Library, European Commission, International Federation of Red Cross and Red Crescent Societies, International Monetary Fund, International Records Management Trust, National Institute of Standards and Technology, NATO, UNESCO, University of British Columbia, University College London, and University of Washington. In order to ensure that the cross-disciplinary nature of the researchers utilize a common foundation for across all the teams, the ITrust project will build upon the findings of the first three phases of the InterPARES research project (1998-2012) by expanding upon those findings with additional case study research, current literature, legislature and regulatory review, and exploratory research.

The ITrust project has been organized into five primary domain areas considered to be of particular interest to the creation, handling, management and storage of digital records in Cloud-based environments, as well as five cross-domain areas.

The five research domains are:

- **Infrastructure:** This domain considers issues relating to system architecture and related infrastructure as they affect records held in online environments. Examples of areas to be investigated include such topics as: types of cloud and their reliability; types of contractual agreements (service level agreements or SLAs) and their negotiation, coverage, flexibility, etc.; costs, up front and hidden.
- **Security:** The security domain considers records issues relating to online data security, including: security methods (encryption, sharding, obfuscation, geographic location); data breaches; cybercrime; risks associated with shared servers; information assurance; governance; audits and auditability; forensic readiness; risk assessment; and backup.
- **Control:** The control domain differs from the security domain in its focus on the management of digital material in online environments. It addresses such issues as: authenticity, reliability, and accuracy of data; integrity metadata; chain of custody; retention and disposition; transfer and acquisition; intellectual control, and access controls.
- **Access:** The access domain researches open access/open data; the right to know/duty to remember/right to be forgotten; privacy; accountability; and transparency.
- **Legal:** The legal domain considers issues such as: the application of legal privilege (including the issue of extra-territoriality); legal hold; chain of evidence; authentication of evidence offered at trial; certification; and soft laws (in particular UN standard-setting instruments) - mapping, scope, potential impact, and constraints;

and the five research cross-domains are:

- **Terminology:** This cross-domain is concerned with the ongoing production of a multilingual glossary; a multilingual dictionary with sources; ontologies as needed; and essays explaining the use of terms and concepts within the project.
- **Resources:** This cross-domain is concerned with the ongoing production of annotated bibliographies, identifying relevant published articles, books, etc., case law, policies, statutes, standards, blogs and similar grey literature.
- **Policy:** The policy cross-domain considers policy-related issues emerging from the five research domains; for instance, it would cover policy issues pertaining to the development and implementation of the 'nfrastructure' or 'security' standards, or as the facilitator for the implementation of laws. In general, it addresses recordkeeping issues associated with the development and implementation of policies having an impact on the management of records in an online environment; policies can be broad, such as a national policy on information management, or very specific, such as a policy on adopting certain standards within an organization.
- **Social/Societal Issues:** This cross domain is concerned with the analysis of social change consequent to the use of the Internet, including but not limited to use/misuse of social media of all types, trustworthiness of news, data leaks (intentional or accidental/force majeure) consequences, development issues (power balance in a global perspective), organizational culture issues, and individual behaviour issues.
- **Education:** This cross-domain is concerned with the development of different models of curricula for transmitting the new knowledge produced by the project [12].

4 Preservation Services for Online Environments

With the adoption rate of Cloud services outpacing legislation and case law, there exists a strong need for a clearly articulated set of functional requirements defining records-related services that support the presumption of authenticity within an online environment. Under the ITrust Control Domain, *Preservation as a Service for Trust* (PaaST) seeks to develop a preservation model that expresses actions and attributes capable of supporting the authenticity of records that are created, managed or stored within Internet-based environments. The purpose of PaaST [13] is to: …provide insight and guidance to both those who entrust records to the Internet and those who provide Internet services for the records. The project will address relevant requirements, insights and concerns developed in other ITrust projects to enrich and strengthen its models. To provide a strong foundation for the proposed preservation services, the PaaST project team is leveraging the Chain of Preservation [14] model developed by InterPARES2. The CoP model stipulates that preservation activities begin with the creation of the record and must be continuously managed throughout the lifespan of that record. As a record moves from creation to active and then inactive stages of its lifecycle, the actions and attributes that are needed at a specific stage to support the record's authenticity also change.

As the services are being written with Cloud Based Services in mind, rather than speaking in terms of preservation environments, the services use the concept of Preservation Environment. As such, PaaST introduces a new set of terminology and information concepts that borrow and adapt from existing standards (OAIS, for example). This concept refers to the highest level of set of Preservation Targets (those objects that are to be preserved by the Preserving Party) under the

Preservation Rules, together with the technological infrastructure and tools necessary to perform the functions specified in the services. The services are structure to be performed independently, be a single provider, or 'farmed' out to a series of providers depending on the needs of the organization. PaaST requirements address the preservation of digitally stored information and at the top level of the hierarchy is the Information Object. To provide a very brief overview of the hierarchy of information objects as viewed by PaaST (see Figure 1: Classes of Information Objects). Information Objects are comprised of Data Objects and Intellectual Objects. Data Objects are what are traditionally understood as the 'digital file', or an ordered set of numbers, characters, signs or other information encoded as binary bits. The Intellectual Object, on the other hand, is a human recognized object (the 'Record') comprised of one or more data objects along with related information and preservation targets. Related Information contains description information about the record in the form of submission information, preservation description information, preservation rules, or heuristic information. Finally, the Preservation Target is the focus of the preservation operation, and is comprised of the zero or more data objects and zero or more related information. Below this Preservation Target are additional Archival Aggregation objects that are beyond the scope of this paper, but these concepts (as well as those briefly touched on above) are covered in much greater detail with the PaaST specification.

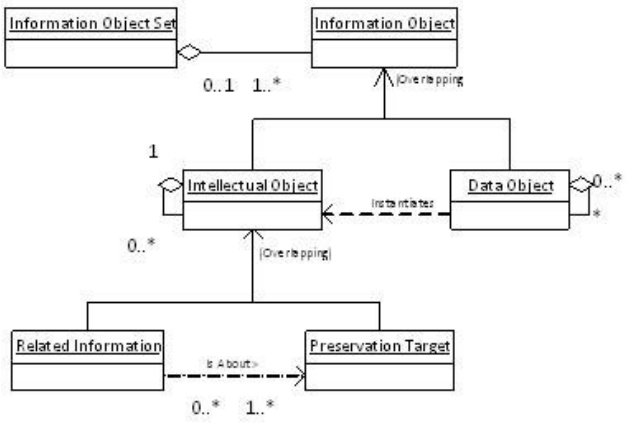

Figure 1: Classes of Information Object

4.1 Preservation Services

To reflect this changing nature, PaaST has identified four distinct services to be modelled:

4.1.1 Receive Submission. The Receive Submission Service ensures that a set of records transferred to an Internet-based environment is complete and intact, and is in compliance with any agreements that are in force between the transferring party and the receiving preservation party (e.g. a Cloud Service Provider).

4.1.2 Preservation Storage. The Preservation Storage service captures, reports and makes available those attributes concerning the storage of the records, the movement within the storage system, and the replacement or upgrade of storage media and related technologies.

4.1.3 Preservation Change. The Preservation Change service captures, reports and makes available those attributes related to the migration, conversion or transformation of the digital objects that constitute a preserved record or the software used to translate the digital bits into a human readable form.

4.1.4 Access. The Access service provides retrieval and production of copies of records and assessment of the authenticity of the copies provided to the requestor.

4.2 Supporting Capabilities

In addition to the Preservation Services, PaaST will provide three categories of supporting capabilities to supplement the Preservation Services.

4.2.1 Management. The Management category is comprised of the Control and Problem Handling capabilities

4.2.1.1 Control. The Control capability is responsible for the determination of which Preservation Rules and Conditions apply to specific cases and enforces said conditions on objects, processes, parties and information.

4.2.1.2 Problem Handling. The Problem Handling capability is responsible for recognizing problems related to objects, processes, parties and information, for characterizing and rating the severity of the problem, assigning resolution of the problem to specific party and tracking problem resolution.

4.2.2 Information Processing. The Information Processing category is comprised of the Information Management, Reporting, Class Definition, Composition Definition, Characterization, Permanent Feature Designation, and Assignment capabilities.

4.2.2.1 Information Management. The Information Management capability is responsible for creating and maintaining Preservation Management Information about the controls, objects processes and parties. Includes categorizing information, extracting data from information sources, generating data from preservation actions and collecting data from inspecting and verification of preservation objects.

4.2.2.2 Reporting. The Reporting capability is responsible for producing, sending and managing reporting functions about objects, processes, parties, and problems.

4.2.2.3 Class Definition. The Class Definition capability is responsible for definition of the composition of objects and their features, as well as establishing the conceptual framework for managing the Preservation Targets along with Related and Linked Objects.

4.2.2.4 Composition Definition. The Composition Definition capability is responsible for identifying the composition of Submission Sets and Preservation Targets and confirming that they meet the specified criteria.

4.2.2.5 Characterization. The Characterization capability is responsible for specifying those features that either individual or

sets of Preservation Targets possesses, or should possess, and, optionally, the values of those features. Information about the Preservation Targets may be derived from a variety of sources, including, but not limited to, Preservation Agreements, Preservation Service Contracts, Submission Information, Linked and Related Data Objects, information derived from Inspection, Verification and/or Authenticity Assessment.

4.2.2.6 Permanent Feature Designation. The Permanent Feature Designation capability is responsible for determining the essential requirements for preservation of a class set, individual Preservation Target, or Preservation Data Object by identifying those features that must remain unchanged throughout the preservation storage and retrieval process.

4.2.2.7 Assignment. The Assignment capability is responsible for assigning individual objects to categories. Categories are assigned via criteria as defined in Class Definition and Composition Definition capabilities based on information about the object and captured as Preservation Management Information.

4.2.3 Object Processing. The Object Processing category includes the capabilities of Inspection, Verification and Authenticity Assessment

4.2.3.1 Inspection. The Inspection capability is responsible for specifying the methods to be used to examine Data Objects in order to identify the components of a composite object, such a Preservation Object, Preservation Aggregate, or Submission Set, or to determine whether the Preservation Target under examination has a particular feature or specific value for a given feature.

4.2.3.2 Verification. The Verification capability is responsible for providing confirmation of existence and values of features of Preservation Targets by comparing information from different sources or information obtained by inspection at different times; also responsible for verifying the success of Preservation Processes, such as Submission and Change.

4.2.3.3 Authenticity Assessment. The Authenticity Assessment capability is responsible for determining the authenticity of Preservation Targets at the time it enters the Preservation Environment, capturing data about the authenticity of Preservation Objects, comparing authenticity related data, and reporting discrepancies in authenticity data.

5 Specification to Standardization

The penultimate goal of the PaaST project is to release the specification to a standards body to have it reviewed, analyzed, and, ideally, approved as an internationally agreed upon standard. To realize this goal, InterPARES has joined the Object Management Group (OMG) and will be working as a member of this standards body to introduce and advance the PaaST specification. The OMG is an international, non-profit technology centric standards consortium whose mission to to:

...develop, with our worldwide membership, enterprise integration standards that provide real-world value. OMG is also dedicated to bringing together end-users, government agencies, universities, and research institutions in our communities of practice to share experiences in transitioning to new management and technology approaches like Cloud Computing [15].

In support of this mission, OMG hosts organizations such as the Cloud Standards Customer Council (CSCC) and the Consortium of IT Software Quality (CISQ) at its quarterly technical meetings in order to: increase industry exposure to technical specifications that are working their way through the OMG approval process, foster cross-sector collaboration, and encourage inter-domain knowledge sharing between organizations.

The standardization process developed by OMG differs from that used by most other standards bodies in that OMG employs a strict "No Shelf-ware" policy; that means that all specifications that are submitted to the OMG for review must have a working product that has been created in accordance with the specification, and therefore validates the clarity and comprehensiveness of the specification, before it will be approved. This requirement to test the implementability of the specification ensures that, upon approval, that the standard is immediately usable without further modification – or that it won't just 'sit on the shelf'. OMG support for specifications continue after approval as well, with OMG producing educational book, training workshops, certification mechanisms. Among the better known OMG approved specifications are several modelling languages widely used within the software and system development sector: Unified Modeling Language (UML), System Modeling Language (SysML), and Model Driven Architecture (MDA).

Working closely with both public and private sector organizations allows for small vertical industry-oriented standards bodies, consortia and other groups (such as research projects like InterPARES) to work alongside the OMG to create and test the metamodels, Applications Program Interfaces (APIs) and other types of specifications that are designed by, and meant by, specific sectors or industries. While the OMG has focused predominately on producing highly technical and widely used specifications that have cross industry applications (such as UML), as a whole OMG relies upon input and feedback from current and new consortia members to address emerging challenges that affect specific sectors that might be outside their normal purview – such as the challenges faced when storing and preserving digital records in Cloud-based environments that ITrust is researching. In order to foster such cross-pollination of sector-specific knowledge and experience, the OMG maintains reciprocal membership agreements and exchanges with industry organizations in encourage industry specific organizations to bring their challenges and concerns to the OMG; among the groups with cross memberships exchange are: Association of Information and Image Managers (AIIM), Open GIS Consortium, Integrated Justice Information Systems (IJIS) Institute, and World Wide Web Consortium (W3C).

Among the benefits to ITrust of working with the OMG to develop PaaST into a publicly available specification is that, in addition to having access to and review by the many

professional and private organizations that participate in the OMG, the OMG also maintains close working relationships with other major global standards bodies in order to reduce duplicative efforts. By maintaining a formal liaison with other standards bodies that publish in similar areas, the OMG can work in concert with these other standards bodies to reduce the number of redundant and occasional conflicting standards issued by different standards bodies. Among the groups with which the OMG works are:: International Organization for Standardization (ISO), European Computer Manufacturers Associations (ECMA), Institute for Electrical and Electronics Engineers (IEEE), and two Accredited Standards Committee (ASC) committees -- X12 (electronic data interchange) and T1M1 (network management). Of particular importance to the PaaST project is the special relationship that the OMG has with International Organization on Standards (ISO). Specifications that are approved by the OMG are recognized by ISO as Publicly Available Specifications; this special recognition allows them to be fast tracked by the ISO Committee on Information Technology Standards (ISO/IEC JTC1) directly onto a final ballot for approval for ratification as an ISO standard.

6 Next Steps for PaaST

The Preservation Services and supporting capabilities that are part of the specification comprising PaaST are still in the design phase of a two-year development cycle. An initial draft of the functional specification for the services and supporting capabilities has been creating, along with functional specifications detailing required and optional functionality. Throughout the development process, researchers from other domains within the ITrust project provide feedback on the PaaST work product as it impacts areas of their own research, as well as propose additional services and/or functional specifications as the needs are identified. Once the ITrust review has been completed, PaaST will be formatted as an OMG Request for Proposal and forwarded to the OMG's Government Information Sharing and Services Domain Task Force for review. The OMG RFP will provide all the information necessary to software developers interesting in creating a functional application that performs all the operations that are detailed within the suite of Preservation Services – i.e. create software based on the PaaST specifications with nothing more than the RFP as guidance. The RFP, as stated in *The OMG Hitchhiker's Guide* [16], is:

… a statement of industry need and an invitation to the software supplier community to provide a solution, based upon requirements stated within. The process of identifying need is a culmination of experience within an OMG technical group…and solicitation of industry recommendation. While the RFP is not prescriptive in the sense of dictating how the solution is presented, it does provide guidelines – requirements – that again are derived from the sources noted above.

Contained with the PaaST RFP will be functional requirements, pre-conditions that must exist for a service to functional, and main and alternate workflows for each of the preservation services; along with appropriate UML Class diagrams of the methods and attributes corresponding to the functional requirements as well as any other supporting material deemed to be helpful to software developers. Should the RFP meet the high standards set by the OMG set by the OMG GovDTF and be approved for released, the RFP will be issued and any OMG member organization may develop and submit a package based on the RFP for evaluation by the group. Based on the quality of the submissions received, the RFP will then be forwarded for full approval as an OMG specification, or require further revision to address any shortcomings that were discovered by the developers who attempted to implement the specification as written.

7 Conclusion

The objective of InterPARES TRUST project is to generate the methodological and theoretical frameworks necessary to support the development of an integrated network of policies, procedures, regulations standards and legislation that can be applied consistently across the broad spectrum of juridical boundaries that exist in the study. The goal is to increase public trust in records stored with Cloud based providers by creating such frameworks grounded on evidence of good governance, a strong digital economy, and a persistent digital memory. In support of that goal, the Preservation as a Service for Trust (PaaST) project is developing a series of preservation services that supports the presumption of authenticity of records entrusted to the Cloud-based Service Providers. These preservation services detail those actions and attributes that need to be documented as records are moved through space, such as transmitted from the creator to Cloud-based Service Provider, or across time, such as being stored in the Cloud for an extended period of time. By implementing the preservation services articulated by PaaST into a Cloud-based storage environment, the record keeping system will capture and document metadata that allows for the identity of that record to be established and its integrity demonstrated within a documented chain of custody. To ensure that the PaaST preservation services can be fully integrated into existing Cloud-based environments, InterPARES is partnering with the Object Management Group to developed PaaST into a working prototype for assessment by the GovDTF and, if found to be accurate, complete and implementable, approved by OMG as a Publicly Available Specification.

Acknowledgements

PaaST has been a major undertaking, started in 2014, that has involved the efforts of many brilliant minds: researchers Dr. Luciana Duranti, Dr. Kenneth Thibodeau, Dr. Giovanni Michetti, Dr. Corrine Rogers, Dr. Joseph Tennis, Adam Jansen, Courtney Mumma, and Daryll Prescott, Katherine Timms, and Graduate Research Assistants Lois Evans, Mel Leverich and Shyla Seller. Primary funding for The InterPARES Trust Project has been provided by the Social Sciences and Humanities Research Council (SSHRC) of Canada through a Partnership Grant. Matching funds

for the project have been provided by The University of British Columbia's Vice President of Research, the Dean of Arts, and the School of Library, Archival and Information Studies. Additional matching support in kind has provided by the over 70 partners participating in this research project. InterPARES Trust is also a partner on the SSHRC-funded Participedia Project led by Dr Warren of the UBC Department of Political Science.

References

[1] Alois Mary, Peter Putz, Dirk Wallerstorfer, Anna Gerber. 2017. *Cloud-Native Evolution*. O'Reilly Media, Sebastopol, CA. ISBN: 978-1-491-97396-7

[2] Chip Walter. Kryder's Law. *Scientific American*. August 1, 2005

[3] Peter Mell, Timothy Grance. 2011. *NIST Special Publication 800-145: The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. Gaithersburg, MD.

[4] United State Government. 2001. Public Law 107-56, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001''

[5] Luciana Duranti, Corinne Rogers. 2012. Trust in Digital Records: An increasingly Cloudy Legal Area. *Computer Law & Security Review*. Vol. 28 No. 5, pp. 522-531.

[6] InterPARES2. Terminology Database, InterPARES. [online]. http://www.interpares.org/ip2/ip2_terminology_db.cfm

[7] Heather MacNeil. 2000. Providing Grounds for Trust: Developing Conceptual Requirements for the Long-term Preservation of Authentic Electronic Records. *Archivaria*, No. 50, pp. 52-78.

[8] Administrative Office of the United States Courts. 2013. *Federal Rules of Evidence*. United States Government. [online]. http://www.uscourts.gov/uscourts/rules/rules-evidence.pdf.

[9] Terry Eastwood. 1994. What is Archival Theory and Why is it Important. *Archivaria*, No. 37, pp. 122-130.

[10] Authenticity Task Force. 2002. *Authenticity Task Force Final Report*. InterPARES. [online]. http://www.interpares.org/display_file.cfm?doc=ip1_atf_report.pdf.

[11] InterPARES Trust. 2013. *InterPARES Trust*. InterPARES. [online] http://interparestrust.org/trust.

[12] InterPARES Trust. 2013. *InterPARES Trust Research*. InterPARES. [online]. http://interparestrust.org/trust/about_research/domains.

[13] InterPARES Trust. 2013. *Research – Studies: Abstracts*. InterPARES. [online]. http://interparestrust.org/trust/about_research/studies.

[14] Terry Eastwood, B. Ballaux, R. Mills, Randy Preston. 2008. Appendix 14: Chain of Preservation Model Diagrams and Definitions. In *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*; Duranti, L. & Preston, R., Eds.; Associazione Nazionale Archivistica Italiana: Padova, Italy.

[15] Object Management Group. 2014. *About the Object Management Group*. Object Management Group. [online]. http://www.omg.org/gettingstarted/gettingstartedindex.htm.

[16] Object Management Group. 2008. *The OMG Hitchhiker's Guide: A Handbook for the OMG Technology Adoption Process, Version 7.8 (omg/2008-09-02)*. Object Management Group, [online]. http://www.omg.org/cgi-bin/doc?omg/08-09-02.pdf.