Trusting records: 20 Years of InterPARES Research

Luciana Duranti, Project Director and Professor
School of Library, Archival and Information Studies
The University of British Columbia
Havana, Cuba 18 February 2019
The Goal of InterPARES 1 and 2 (1998-2006)

To develop the body of **theory** and **methods** necessary to ensure that digital records produced in **databases** and **office systems** as well as in **dynamic, experiential and interactive systems** in the course of artistic, scientific and e-government activities can be created in **accurate** and **reliable** form and maintained and preserved in **authentic** form, both in the long and the short term, for the use of those who created them and of society at large, regardless of technology obsolescence and media fragility.
Goal of InterPARES 3 (2007-2012)

- To **enable** public and private **archival organizations and programs** with limited resources **to preserve** over the long term **authentic records** that satisfy the requirements of their stakeholders and society’s needs for an adequate record of its past.

- It did so by building on the products of the first two phases of InterPARES (1998-2006)
Policy Framework

A framework of principles guiding the development of policies for records creating and preserving organizations
IP 1 & 2 Products

Creator Guidelines

Recommendations for making and maintaining digital materials for individuals and small communities of practice
IP 1 & 2 Products

Preserver Guidelines

Recommendations for digital preservation for archival institutions
IP 1 & 2 Products

Benchmark and Baseline Requirements

Authenticity requirements for assessing and maintaining the authenticity of digital records

**Requirement Set A**

To support a presumption of authenticity, the preserver must obtain evidence that:

**Requirement A.1:** Expression of Record Attributes and Linkage to Record

The values of the following attributes are explicitly expressed and derivable linked to every record. These attributes can be distinguished into categories, the first concerning the identity of the records, and the second concerning the integrity of records.

- **A.1.a** Identity of the record:
  - Names of persons concerned in the formation of the record:
    - Name of author
    - Name of writer (if different from the author)
    - Name of originator (if different from name of author)
    - Name of address
  - Name of action or matter
  - Dates of creation and transmission, that is:
    - Chronological data
    - Received data
    - Archival data
  - Transmission data(s)
  - Indication of attachments

- **A.1.b** Integrity of the record:
  - Name of handling office
  - Name of office of primary responsibility (if different from handling office)
  - Indication of types of annotations added to the record
  - Indication of technical modifications

**Requirement A.2:** Access Privileges

The creator has defined and effectively implemented access privileges, modification, annotation, relocation, and destruction of records.

**Requirement Set B**

The preserver should be able to demonstrate that:

**Requirement B.1:** Control over Records Transfer, Maintenance, and Reproduction

The procedures and system(s) used to transfer records to the archival institution or program must maintain them, and reproduce them by adequate and effective controls to guarantee the records' identity and integrity, and specifically that:

- **B.1.a** Unbroken custody of the records is maintained;
- **B.1.b** Security and control procedures are implemented and monitored; and
- **B.1.c** The content of the record and any required annotations and elements of documentary form remain unchanged after reproduction.

**Requirement B.2:** Documentation of Reproduction Process and its Effects

The activity of reproduction has been documented, and this documentation includes:

- **B.2.a** The date of the records' reproduction and the name of the responsible person;
- **B.2.b** The relationship between the records acquired from the creator and the copies produced by the preserver;
- **B.2.c** The impact of the reproduction process on their form, content, accessibility and use; and
- **B.2.d** In those cases where a copy of a record is known not to be fully and faithfully reproduce the elements expressing its identity and integrity, such information has been documented by the preserver, and this documentation is readily accessible to the user.

**Requirement B.3:** Archival Description

The archival description of the form containing the electronic records includes—in addition to information about the records' juridical-administrative, provenience, procedural, and documentary contexts—information about changes the electronic records of the creator have undergone since they were first created.
IP 1 & 2 Products

File Format Selection Guidelines
Principles and criteria for adoption of file formats, wrappers and encoding schemes
IP 1 & 2 Products

Terminology Database
Including a glossary, a dictionary and ontologies
IP 1 & 2 Products

Two Records Management Models

Chain of Preservation (COP) Model (lifecycle)
Business-driven Recordkeeping (BDR) Model (continuum)
IP 1 & 2 Final Products

Two books:


InterPARES 3 General Studies

- National Standards Relevant to IP3
- Community Archives e-Records Assessment
- Public Sector Audit Report for Digital Recordkeeping
- Records Management Policies and Procedures Template
- Cost-benefit Models
- Ethical Models
- File Viewers
- **Education Modules**
- Open Source Records Management Software
- Metadata Applications Profiles
- Organizational Culture & Risk Assessment
InterPARES 3 General Studies

- Web 2.0/Social Media
- **Terminology Database**
- Analysis of Other Digital Preservation Projects
- International Standards Relevant to IP3
- Annotated Bibliography Database
- E-mail Preservation
- Preservation of Registries
InterPARES Products

All InterPARES 1-3 Products are available at

www.interpares.org
Increasingly individuals and organizations choose to keep their records online. The primary uses of the online environment are:

- Backup
- Collaboration
- Distribution (including social media)
- Recordkeeping
- Long-term storage
- Keeping Archives
Internet providers are “entities providing users the ability to communicate through a computer system that processes or stores computer data on behalf of such communication or users.” (Budapest Convention on Cybercrime, 2001). Three “actions” relate to the definition of provider: communication, data processing and data storage.

Cloud computing is a “model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” (National Institute of Standards and Technology, 2009)

The services offered by Internet and Cloud Providers are not regulated or transparent.
Trust on the Internet or Cloud

- The **standard of trust** online is that of the ordinary marketplace, *caveat emptor*, or **buyer beware**

- **What is trust?**

- Some view it as a four-level progression: from **individual**, as a personality trait, to **interpersonal**, as a tie directed from one person to another (son to father); to **relational**, as a property of a mutual relationship (people doing business); and **societal**, as a feature of a community as a whole.
InterPARES Definition of Trust

- InterPARES defines trust as confidence of one party in another, based on alignment of value systems with respect to specific actions or benefits, and involving a relationship of voluntary vulnerability, dependence, and reliance, based on risk assessment.

- Substantially, trust involves acting without the knowledge needed to act, by substituting the information that one does not have with other information, e.g. the testimony of witnesses, oral tradition, documentary evidence.
Questions to Ask Providers

- How can a confidentiality of information be protected?
- How can a human or legal person’s privacy be protected?
- How can an organization’s forensic readiness be maintained and compliance with the law ensured?
- How can an organization’s records’ accuracy, reliability, and authenticity be guaranteed and verifiable?
- How can an organization’s records and information security be enforced?
- How can an organization maintain governance upon the records entrusted to the Internet or the Cloud?
- How can the preservation of records of permanent value be ensured?
The Classic Response

- Choosing to keep records online is a **Risk Assessment** decision where Risk = probability x impact. It is a question of comparison. If one cannot have everything, what does one give up?

- The first choice offered us is **between Transparency and Security**: providers offer trust through technology and location independence.

- The second choice offered us is **between Control and Economy**: Providers offer trust through control on expenditures.
If we decide to carry out our activities online, we must find a balance between trust and trustworthiness, which is needed to ensure a balanced trust relationship.

Trust constitutes a risk which can only be mitigated by the establishment of a trust balance: we must trust trustworthy trustees and trustworthy records.
The goal of InterPARES Trust was 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 online, to ensure public trust.

InterPARES Trust has been funded by a SSHRC Partnership grant and matching funds from UBC and all the partners (in cash and/or in kind)
InterPARES Trust Participants

- The **International Alliance** comprises 7 Teams:
  - North America
  - Latin America
  - Europe
  - Asia
  - Australasia
  - Africa
  - Transnational Organizations

- Supporting Partners
- Pro-bono Consultants
- Management Team

A total of 490 researchers in 42 countries
Partners

- Universities
- National & Regional Archives
- Libraries
- Governments
- International Organizations
- Businesses
- Individual researchers
Methodology

- Archival and diplomtics methods
- **Resource-based theory** because of the need to understand the technologic, managerial and relational means of maximizing competitive advantage
- **Risk management** because of the need to identify vulnerabilities and ways to mitigate them
- **Design theory** because of the need to develop policy in situations with unknown variables
- **Digital forensics**, because of the need to assess the authenticity of digital materials that do not reside in the systems in which they were produced and kept
- **Human computer interaction; aero-spatial, cybercrime, and telecommunication law; organizational theory**, etc.
Research Domains

- Infrastructure
- Control
- Legal Issues
- Access
- Security
Access

13 studies

UK Case studies: care.data Programme; National Health

NA: RM in Open Gov, Data, Big data
NA: Patents and Petitions

AA: Trusted online access to distributed holdings of digital public records

UK: RM in Open Gov
Sweden: RM in Open Gov

AA: Te Reo Maori
EU: Internet Archives Russia
Control

32 studies

Enterprise:
Supporting business processes; audit

RM & Preservation;
PaaST; TRUSTER

Government:
Retention & disposition; web analytics; open gov; big data

Health care:
Monitoring IM in hospitals

Heritage:
Interoperability of metadata
Security

- NA: Standard of Practice for archives
- TR: Security Classification (checklist)
- NA: Privacy/Security Techniques
- TR: Use of Cloud in international organizations

4 studies
Infrastructure

10 studies

South Africa: RM in networks
Croatia: Trusted IaaS
AA: Dark Repositories as a Service

Asia: Trusted certification
NA: Contract terms for cloud services
EU: Economic models for cloud storage decisions
EU: Benefits realization management
AF: Enterprise digital RM (3 locations)
Legal issues

NA: Checklist for evaluating cloud contracts
EU: Impact of Italian legal framework
AS: Policies, legislation, standards for RM in the cloud
NA: Comparison among legal issues in the ITRust Regions
NA: Database of privacy case law

Legal 5 studies
Research Cross-Domains

- Resources
- Policy
- Social issues
- Education
- Terminology

Research cross-domains
Policy

- EU: Girona City Council
- EU: Info governance maturity – Phase 1 & 2
- AS: Access to government info, Malaysia
- EU: Analysis of policies for RK & preservation
- NA: Policy & plurality
- NA: Retention & Disposition
- AA: Digital preservation in the cloud

Policy 8 studies
Social Issues

AS: Social awareness of authenticity
AS: Government information in China
AS: Security awareness in Korea
NA: Social media and trust in government
EU: Ethical foundations of preservation
EU: Materiality of records and attributes of trust
NA: Org culture ‘Fun in Functional’
NA: Historical Study of Cloud
NA: Documentary
LA: Records in the cloud, Mexico

Social issues 10 studies
Resources & Education

- Terminology Database
- Literature reviews
- Ontology of functional activities for archival systems (TR)
- Reports (NA)
  - Notes on International Law
  - Trust in Law
  - Trust in Business
  - Trustworthy Smart Grid Infrastructures
- Review and update of Digital Records Pathways (AA/NA)
- Curriculum Alignments at Institutions of Higher Learning in Africa (AF)
Research Dissemination is authored by InterPARES Trust researchers and research assistants. They will be listed below on an ongoing basis.

Search

by Author: 

by Text in Citation: 

Search

Publications

[ 17 ] Books (Including Chapters)
[ 53 ] Articles - Refereed
[ 117 ] InterPARES Trust Research Documents
[ 5 ] Theses

Presentations

[ 62 ] Lectures, Workshops, and Seminars
[ 178 ] Conferences (Symposia, Sessions, Panels, Papers)

Public Relations

[ 20 ] Articles and Reviews
[ 7 ] Broadcast Interviews
[ 5 ] Reports
[ 2 ] Sponsorships
[ 2 ] Videos
The Books!


12 chapters covering the main findings of the project that are relevant to all cultural and juridical environments.

By Routledge, Taylor and Francis Group:
- A book by the African Team
- A book by the European Team
- A book by the Transnational Team
THANK YOU

www.interparestrust.org

luciana.duranti@ubc.ca