Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

SI 655
Management of Electronic Records

Week 03

February 2, 2009

Trust in Records and Recordkeeping Systems

Outline

- Bantin review essay - debates and reflections/positions
- Trust
  - electronic commerce
  - technical needs
  - traceability
  - limitations
- Authenticity
  - MacNeil
  - Lynch
  - integrity
  - digital signature issues
- Trust and Authenticity
  - risk assessment
  - trusted repositories
  - user behavior and authenticity

Bantin review essay

- Debates/Issues
  - Defining the "record"
  - Identification & appraisal
  - Documentation (Metadata) for authenticity and reliability
  - Electronic recordkeeping systems
  - Preservation / current use
  - Physical custody / access
  - Role on IT development / environment
- Interpretations / positions
- Reflections

Trust

- Where does lack of trust come from?
  - Motivation to deceive
  - Lack of demonstrated competence
  - Lack of track record
  - Absence of accountability
  - Absence of "proof"
  - Lack of familiarity (with the source, process or technology)

Questions

- Does digital information need to be held to a higher standard for authenticity and integrity than printed information?

- Which information?

- Why? Why Not?

Trust in Electronic Commerce (Steinauer et al.)

- Reducing risk
  - Transfer of risk
  - Reduction of liability
- Trustworthy processes
- Traceability
- Intermediaries and Trusted Third Parties
- Endorsements
- Formal Testing and Certification
- Legal Underpinnings and Remedies

Technical Needs

- Secure the system against unauthorized use
  - Identification and Authentication
    - Password protection
    - Smart cards
    - Biometrics
    - Access controls
    - Audit trails & Transaction data (Integrity)
    - Confidentiality
    - Government interest

Traceability

- Physical goods (is what I received what I ordered?)
- Digital goods (is what I received unaltered)
- Source/Supplier (did it come from where I expected it to)
- Recipient (did I send it to who I intended)

Limitations of technical controls for records and recordkeeping systems

- Dependencies
  - Legal requirements (access to encrypted information)
  - Long term maintenance requires changing the objects
  - Long term maintenance of the technical infrastructure

Authenticity (Documentary form - MacNeil)

- Intrinsic Elements (identity)
  - Name of author
  - Name of originator
  - Chronological date
  - Name of place of origin
  - Name(s) of the addressee(s)
  - Names(s) of recipients
- Extrinsic Elements (integrity)
  - Presentation features
  - Electronic signatures
  - Time and date stamps
  - Annotations

Contexts: juridical-administrative; provenancial; procedural; documentary; technological

Authenticity (Lynch) 1...

- Philosophical/social constructs (people)
- Technological constructs (code)
  - Authenticity
  - Integrity

- Need to connect the two

Authenticity (Lynch) 2...

- Object + collection of assertions
- Assertions
  - Internal
  - External
- Object (Has it changed?)
- Assertions (Are they correct?)

Tests for Authenticity

- Forensics
- Diplomatics
- Intellectual Analysis of Consistency and Plausibility
- Evaluation of Truthfulness and Accuracy

Integrity (Lynch)

- Has not been corrupted in transit
  - In delivery / rendering
  - Over time

Testing for Integrity

- Compare to a known "true" copy
- Check digital signature
- Establish integrity of the digital signature

Digital Signature Issues

- Granularity
  - Bit
  - Page
  - Document
  - Object
  - Collection of objects
- Scope
  - Content
  - Signer
  - Role of signer
  - Assertions
- Management over time

Trust and Authenticity

- What should technology do?
- What should people do?

Risk Assessment

- Motivation to deceive
- Lack of demonstrated competence
- Lack of track record
- Absence of accountability
- Absence of "proof"
- Lack of familiarity (with the source, process or technology)

Trusted Repositories

- Goals
- Reducing risk
  - Transfer of risk
  - Reduction of liability
- Trustworthy processes
- Traceability
- Intermediaries and Trusted Third Parties
- Endorsements
- Formal Testing and Certification

What is a "Trusted" Repository?

- Trusted "third party" based on
  - Competence
  - Disinterest in deceit
  - External Certification
- Examples:
  - Digital Notary Service
    - See: http://www.surety.com/
  - G-Mail
  - OCLC Digital Archive Service
    - See: http://www.oclc.org/digitalarchive/default.htm

Attributes of Trusted Repositories

- Compliance with OAIS Reference Model
- Administrative responsibility
- Organizational viability
- Financial sustainability
- Technological and procedural suitability
- System Security
- Procedural accountability

User behavior and authenticity

CAMiLEON Project http://www.si.umich.edu/CAMILEON/

- Users apply complex logic to reason about the probability of authenticity
  - Appearance/presentation
  - Role and background of author
  - The function of an application to support the task
  - Technological environment
  - Trusted Institutions