
Wallace, David A.; Hedstrom, Margaret

http://hdl.handle.net/2027.42/78185
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 04
February 9, 2009

Evidence, Discovery, and Admissibility
Outline

• Evidence
• Electronic records and evidence
• Legal evidence
• Discovery
• Sedona Guidelines
• Federal Rules of Civil Procedure
• DVD: MER 2006: Mock Pre-Trial Conference
This issue of evidence

• Records as “evidence” of transactions
  - Key distinctions between generic information systems and recordkeeping systems
    • Records are created, captured, and set aside in the normal course of business as evidence of transactions
    • Courts and auditing procedures typically use broader definitions of evidence.
Why do organizations create and keep records?

• Organizations keep records for two reasons:
  - Legal Requirements
    • Laws, Regulations, Auditing Requirements
  - Business Needs
    • Critical information, performance monitoring, organizational memory and learning, competitive analysis, precedent, etc.
Paper records and evidence

• Records
  – Content and contextual information (metadata) bound in a single document or system of records
  – Eye-readable

• Records systems
  – Under central control (separation of control from interest in tampering)
  – Organized in systems to support specific business processes
  – Fixed retention periods with disposition plans
Electronic Records & Evidence

• How are electronic records different from paper records?
  – Volume and duplicability
  – Persistence (destroyability / recoverability)
  – Dynamic, Changeable Content
  – Metadata
  – Environment Dependence & Obsolescence
  – Dispersion and Searchability

(Sedona June 2007)
Volume and Duplicability

- 93% of all newly recorded information is on electronic media (70% of which is never converted to hard copy)
- Newly recorded information on paper only is 0.01% of the total
- One-third of electronic information is never printed on paper
- Marginal cost/effort to produce copies is almost 0
Persistence (destroyability/recoverability)

- Long-term retention requires regular maintenance and migration activities
- Deleting information from a system does not ensure that it has been destroyed
  - This is particular problem when information is easy to replicate
Dynamic, Changeable Content

• Purpose of electronic systems: maintain current information
• Ability of update automatically in response to new information
• Ease of overwriting and updating
Metadata

• Key data about records (typically bound to a paper record)

• Electronic Records Metadata
  – System Generated
  – User-generated
  – Internal (embedded)
  – External
Metadata Bound to Physical Records

Declass Authority & Date
Approval Date: 4/21/69
Subject
Participants
Distribution
Content

Declassified State Department memo
Metadata bound to physical records
SECRET STATE 194280

EXDIS

FOLLOWING SENT ACTION TEL. AVIV, SEPT 28, FROM SECSTATE RPTD TO YOU:

QUOTE SECRET STATE 194280

EXDIS

E.O. 11652 - XGDS
TAGS: IS, EG, SY, MOPS
SUBJECT: RUMORED EGYPTIAN MILITARY ALERT

FOR AMBASSADOR FROM SISCO
Environment Dependence & Obsolescence

• Some records need to be retained beyond the life of the systems on which they originate.

• Maintaining records in an external system usually requires changing the records and/or the metadata associated with them.

• Information systems generally are not designed to do this.
Dispersion and Searchability

• Digital records are easy to replicate and alter (change, annotate, etc.)
  – Multiple variants

• Digital records are not organized in institutional / shared systems

• Automated tools make search easy
Legal Evidence
(Giordano, 2004)

• Computer Evidence issues
  – Admissibility
  – Authenticity
  – Completeness
  – Reliability
  – Believability
Legal Admissibility

• Weight vs. admissibility

• “Hearsay”
  – “a statement, other than one made by the declarant while testifying at the trial or hearing, offered to prove the truth of the matter asserted”
  – “Hearsay” cannot be cross-examined

• Exceptions
  – “Business Records” – common or routine products of an organization (produced and used in the normal course of business)
  – Best evidence rule (copies in lieu of the original)

• Computer-generated (fingerprints) v. computer-stored records as solution to not excluding all computerized info? (Wolfson)
Admissibility

Tests

• Business Records Exception
  – Used in the “normal course of business”
  – Relied on for normal activities

• Best evidence rule
  – Copies in lieu of the original
    • Original cannot be found
    • Original was destroyed in a regular and controlled business process
    • Format conversions
Authenticity

• Positively tie the evidence to an incident
  - System used produces an accurate result
  - Not altered or tampered with
  - Corroboration (circumstantial evidence)
Reliability

- Current presumption of legitimacy
- Reliability of software used to create records (**and problems with**)  
- Identifying the author (source)
- Corroborating evidence
  - Cuckoo’s egg case; automatic printouts & log files, connection records; utility programs records; agreement with forensic tools)
Believability

• Circumstantial guarantees of trustworthiness
• Content oriented
• Absence of an incentive to cause prejudice
• Corroboration
Issues

• Business Records Exception
  - Which records are kept in the “normal course of business?”
  - What is the status of computer-generated records that are stored but not kept in a regular fashion?
Discovery

• Request by a party to inspect and copy any pertinent records

• E-discovery covers electronic documents and data (email, web pages, word processing files, databases, etc.)

• Preparation
  – Records retention program
  – Employee education (recordness, retention; retrievability after “destruction; personal emails; spoliation)
  – Format conversion of critical records
  – Catalogs
  – “Persons with knowledge” identified (deposition; interrogatory value)
Sedona Guidelines 1...

- Preserve records in anticipation of litigation
- Proportionality. Balance costs, burden, and need
- Confer early in discovery process
- Discovery requests should be clear and focused
- “Reasonable and good faith effort” does not mean taking “every conceivable step”
Sedona Guidelines 2...

• Responding parties are best able to determine how to comply with requests
• Burden of demonstrating (in)adequacy of production on requesting party
• Access beyond active systems must demonstrate relevancy that “outweigh(s) cost, burden, and disruption”
• Absent demonstrated special need or relevance, respondent not required to “preserve, review or produce deleted, shadowed, fragmented, or residual” ESI
• Respondent to follow “reasonable procedures to protect privileges and objections to production”
Sedona Guidelines 3...

- Electronic tools and processes (sampling, searching, identification criteria) can serve “good faith” obligations
- Production to be in forms/format ordinarily maintained, including metadata to search, retrieve and display
- Review and production costs borne by either requester or respondent depending on “special circumstances”
- Spoliation sanctions mandated only upon finding of “intentional or reckless failure to preserve and produce relevant” information and that such information material to ruling
Federal Rules of Civil Procedure 1...

• Updated and effected December 1, 2006
• Formally align legal process with business reality
• “Electronically Stored Information” (ESI) category. Provides ESI as subject to discovery and production.
Federal Rules of Civil Procedure 2...

• Changes / Issues confronted:
  - Requirement to meet in advance of trial (preserving discoverable information; scheduling discovery)
  - Provide names of holders of relevant information and description of data prior to receipt of discovery request
  - Discovery of information not reasonably accessible (undue burden and cost)
  - Destruction under routine, good faith operations (retention management; safe harbor v. spoliation)
  - Protecting attorney-client / work-product (quick peek; clawback)
  - Subpoenas for ESI (Spiro; www.axsone.com/pdf/FRCP_V8_2007.pdf)
Federal Rules of Civil Procedure 3...

- Implications
  - ERM policies and procedures (legal, IT, RM perspectives) essential
  - Need to be able to demonstrate suitability and enforcement of policies, procedures, and management of ESI
  - IT infrastructure will impact discoverability
  - Where and how ESI stored and managed
  - Who has ESI and where and how retained
  - Abilities to access, search, retrieve ESI in event of litigation

(Spiro; www.axsone.com/pdf/FRCP_V8_2007.pdf)