Legal Uses of Human Rights Documentation
Challenges of Digital Evidence

Human Rights Archives
And Documentation
Columbia University

Lucy L. Thomson, Esquire
October 5, 2007

The Digital World is Exploding

- The Internet has revolutionized communications and made global information systems a reality
- The Digital World is networked
- Information systems are increasingly complex
- They are geographically disbursed -- Remote users with portable computers and cellular modems or wireless access may not have any fixed location.
- Databases use proprietary software
- Encryption is required to protect sensitive and personally identifiable information

New Uses for Human Rights Documentation Impose Greater Demands

- Prosecution
- Reparations
- Excluding Perpetrators from Security Forces
- Preserve Information not only for History, but also for Prosecution
- Requires Interdisciplinary Effort; Seriousness of Purpose

New Forms of Documentation

- Web Sites
- E-mail and Instant Messenger
- Databases and Computer Printouts
- Videotapes
- Podcasts
- Online News Feeds
- Oral Histories
- Digital Photographs
- Voice Mail Recordings
- Forensic Evidence/Medical Records (MRIs, CAT scans, Personal Medical Records (HIPAA))
- Computer-Generated Diagrams and Models
- Data Mining/Business Intelligence
- Biotech/ nanotech are creating new life forms
- Metadata

An Ever-Increasing Array of New Technologies are Creating New Forms of Digital Evidence

- Web Sites
- Computers
- Software
- PDAs
- Cell Phones
- CD Roms/DVDs
- Portable Audio

What Are the Implications for Documentation in the Digital Age?

- "Credible information is one of the most powerful tools that a human rights organization can use to create change."

  --Physicians for Human Rights

Initial Efforts by the Courts to Come to Terms with Digital Evidence

- Amendments to the Federal Rules of Civil Procedure (December 1, 2006)
  - Provide new procedural requirements related to Electronically Stored Information (ESI)
  - Scheduling Conference – Meet and Confer
  - Early in the Lawsuit: Parties to Litigation Must Exchange Information About ESI

Federal Rules for "Electronically Stored Information" (ESI)

- Scheduling Conference – Meet and Confer
  - What electronically stored information (ESI) is available?
  - In what format?
  - What information is not reasonably accessible because of undue burden of production or cost?
  - What information will not be produced?
  - What form and format does requesting party want the data?

Foundations for Digital Evidence in Legal Proceedings is Based on the "Paper" Model

- Federal Rules of Civil Procedure and Evidence
  - Electronic evidence is a key part of discovery
- Authentication -- present proof that the evidence is what the proponent claims that it is
- Best Evidence – applies if the document's terms are at issue; there are no "originals" of digital evidence
- Hearsay – an out-of-court statement introduced for the truth of the matter asserted; is e-mail a statement or a business record?
- Relevance – the evidence must be relevant to the claims asserted

Foundations of Digital Evidence in Legal Procedings -- Authenticity

- Authenticity
  - Evidence is what the proponent claims it to be
- "Traditional" Foundation focused on the relationship between the information and the computer
- Documents were admitted based on the assumption that information produced from a computer is inherently reliable
- Self-Authenticating Records
  - Federal Rules of Evidence -- Rules 902(11) and Domestic Business Records and (12)) Foreign Business Records.

21st Century Foundations of Digital Evidence

- 21st Century Foundations will focus more broadly on the Components of an Information System
  - ❑People
  - ❑Process
  - ❑Technology (hardware and software)
- Show that the information system was correctly designed, configured (firewalls, audit and logging) and maintained (patches)
- Must address the problem that computer records may be altered, forged or otherwise changed by hackers or malicious insiders

Protection of Digital Evidence

- Ensuring the confidentiality, integrity, availability, and privacy of information and data is fundamental to protecting the organization's information assets
- Confidentiality – Protection from Unauthorized Access and Disclosure
  - ❖Interception Threatens Confidentiality
- Integrity – Protection from Alteration
  - ❖Modification of Data Threatens Integrity
- Availability – Of Data and Service
  - ❖Denial-of-Service Threatens Availability

Appropriate Security Features Must Be in Place to Protect the Network

- User Identification and Authentication (I&A)
- User Provisioning/Identity Management
- Authorization and Access Control
- Audit and Logging
- Encryption
- Boundary Protection
- System Monitoring
- Security Incident Handling
- Backup and Recovery

Official vs. Authentic

- Official – Content that is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications
- Authentic – Content that is verified to be complete and unaltered when compared to the version approved or published by the content originator. *Authentication* provides verification that the digital content is authentic or official and certification is provided to users accessing the content with an integrity mark

AALL *State-By-State Report on Authentication of Online Legal Resources* Finds Shortcomings

- Online legal resources are increasingly the sole *official* published source. Laws addressing those resources and other online *official* sources are seriously deficient, failing to require certification as to completeness and accuracy for online resources comparable to that required for print *official* sources.
- Official status demands appropriate authentication procedures. Standard methods of authentication may include encryption, digital signature and public key infrastructure but other methods to adopt best practices are also possible. Certification or other types of formal endorsement of legal resources are a vital link in the 'chain of custody' involved in dissemination, maintenance, and long-term preservation of digital materials. That chain may contain a link to computer technologies that guarantee the very copy delivered to one's computer screen is uncorrupted and complete or it may be part of other archival methods.

-- American Association of Law Libraries (March 2007)

New Government Authentication Solution

- Government Printing Office (GPO) Public and Private Laws [Beta application]
  - ❖Assures users that the information is official and authentic and that trust relationships exist between all participants in electronic transactions
  - ❖Affords users further assurance that files are unchanged since GPO authenticated them
  - ❖Provides authenticated Adobe Portable Document Format (PDF) files for the 110th Congress
  - ❖Contains PDF files digitally signed and certified by GPO using Public Key Infrastructure (PKI) technology

References

- NIST Special Publications
  - 800-53A, Security Controls
  - 800-63, Electronic Authentication Guideline
- Government Authentication Solution
  - GPO Authentication Initiative, Public and Private Laws Beta Application, Authenticated Public and Private Laws, available at http://fdlpdev.gpo.gov/plaws/index.html
- American Association of Law Libraries, *State-By-State Report on Authentication of Online Legal Resources* (March 2007), *available at* http://www.aallnet.org/aallwash/authenreport.html.