Records, Risk, & Digital Records Forensics

Alexandra Allen

Corinne Rogers

Archives Association of British Columbia

Annual Conference

Vancouver, BC, Canada

17 April 2010

Digital Records Forensics Project

The Digital Records Forensics Project is a collaboration between:

- The School of Library, Archival & Information Studies
- The Faculty of Law
- Computer Forensics Division of the Vancouver Police Department

http://www.digitalrecordsforensics.org

Digital Records Landscape

- > 90% of all information is being created in electronic format
- Records are being created and must be maintained and preserved in a rapidly changing technological context
- Documentary evidence called in legal proceedings is increasingly in electronic format

At common law

- Admissibility of documentary evidence is at discretion of presiding judge
- Rests on matters of law: relevance & authenticity
- Documents are hearsay but may be admissible under exceptions
- What does “best evidence” mean in the digital environment?

Law of Evidence

- Documents are hearsay - under what exceptions are they admissible?
  - Business records exception: created in usual and ordinary course of business, and it was the regular practice of the business activity to create them

Law of Evidence

- Best evidence rule required by common law
  - The original is preferred
  - No originals in the digital environment
  - Satisfied on proof of the integrity of the system and authenticity of the record

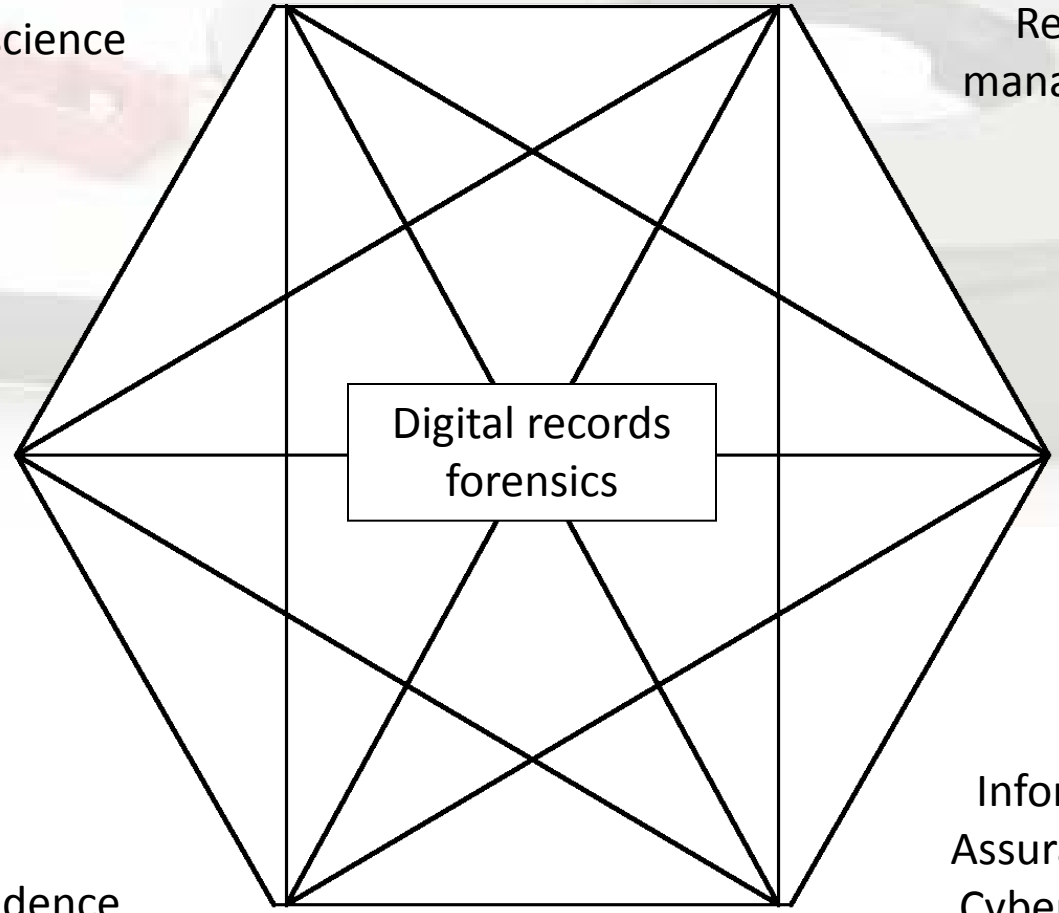
Challenges to digital evidence

- "Digital forensic evidence is challenged by identifying that, by intent or accident, content, context, meaning, process, relationships, ordering, timing, location, corroboration, and/or consistency are made or missed by the other side…"

Frederick B. Cohen

"Fundamentals of Digital Evidence"

Digital Records Forensics



Some definitions

- **Digital Diplomatics:** studies the nature, genesis, formal characteristics, structure, transmission and legal consequences of records
- **Digital Forensics:** scientifically derived and proven methods for the collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence

Records - the archival / diplomatic view:

- any document made or received in the course of a practical activity by a natural or an artificial person and kept for action or reference

Records - The Digital Forensics View

- **Computer Stored**: contain by human statements
- **Computer Generated**: output of a computer program run without human intervention
- **Computer Stored & Generated**: human input followed by computer processing

Static: manifest content & unchanging form
Interactive: variable content &/or form

Non-dynamic: rules of presentation fixed; content from a finite set of data
Dynamic: rules governing content & presentation may vary

How does digital forensics support admissibility?

Digital forensic experts look for **repeatability, verifiability, objectivity** and **transparency** of the ***process***

Daubert Guidelines

- Testing
- Error rate
- Publication
- Acceptance

Digital *records* forensics

- Archival concepts of authenticity and reliability can be brought to bear on admissibility and weight (relevance) of *evidence* respectively
- Archival theory places *records* in context
- Diplomatic theory examines *records* as individual items

Some preliminary interview findings

- Preservation requirements and/or expectations are longer, becoming indefinite, but the means are unclear
- The courts still have paper minds
- Lack of consistency in understanding of digital issues
- Records are whatever is presented as evidence

For example…

The issue of **what is a record in the digital environment** keeps coming up at trials and in political discussions.

- British Columbia Rail case: “What is the definition of a record?” and “what extent e-mails qualify [as records]” (Vancouver Sun, January 29, 2010)
- The Supreme Court of Canada will be hearing a defamation case on whether hyperlinks in a text constitute a repetition of a defamatory statement (Vancouver Sun, April 2, 2010).

Forensic readiness

- Forensic investigations are “post-event”
- Forensic readiness anticipates an information security incident or litigation hold
- Forensic readiness is the process of maximizing potential to use digital evidence & minimizing disruption and cost of investigation

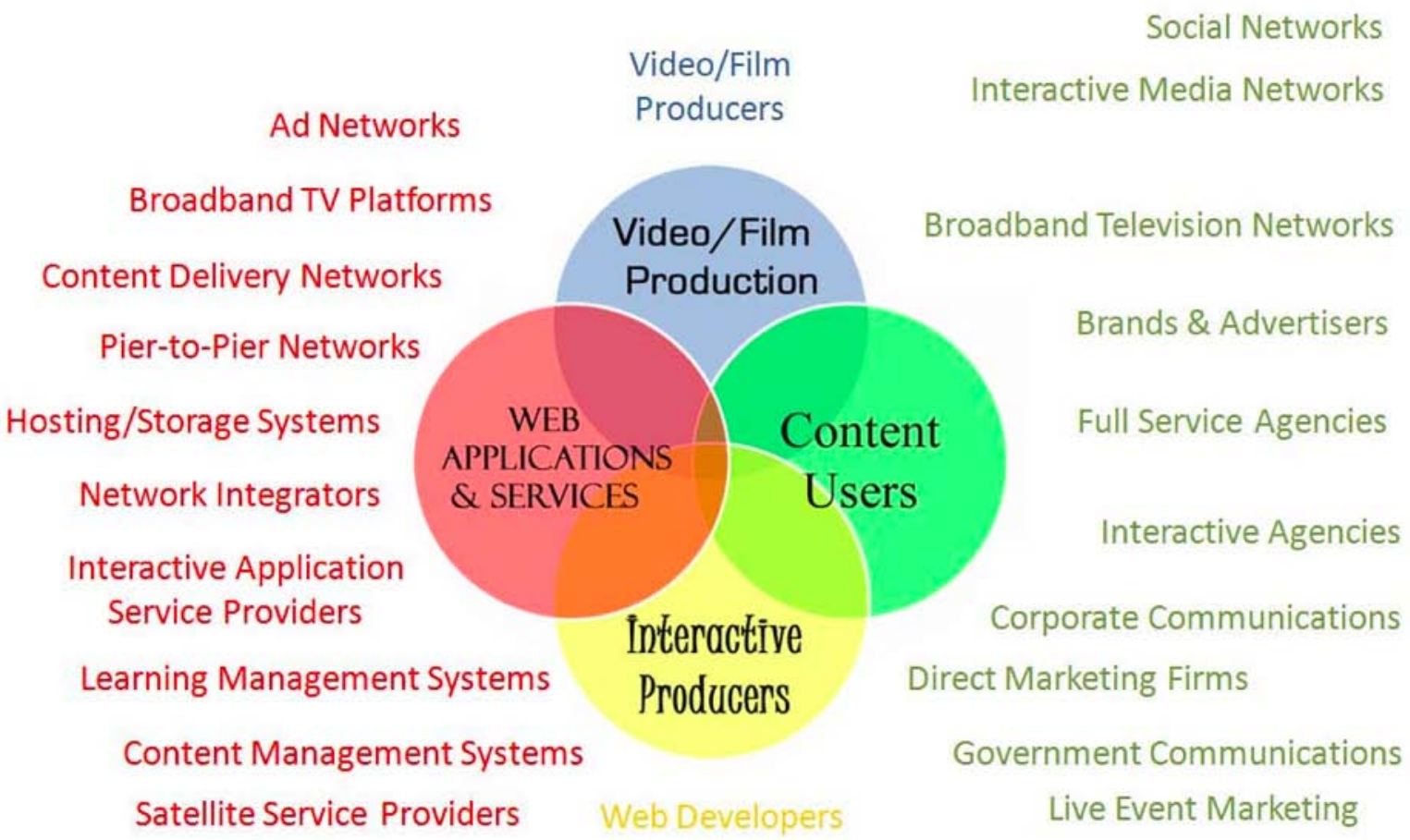
Risk

- "…the systematic application of policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating, and monitoring risk." DIRKS

In a Local Context - VPD

- Chain of custody is the basis for presumption of reliability and authenticity.
- Complete reliance on EDRMS to make explicit all links between records
- Retention schedule exists but is not fully implemented

DIGITAL MEDIA ECOSYSTEM



Treliosdmg.com