# Digital Traces as Sources of Evidence & Memory

Jessica Bushey, PhD Candidate
iSchool @ University of British Columbia
jbushey@mail.ubc.ca

## Introduction

The global adoption of mobile phones with Internet connectivity is changing the way organizations and individuals create, share, reuse, and store their business records and personal communications. The adoption of online services, such as social media platforms that utilize cloud-computing to deliver 24/7 access, collaborative tools and scalable solutions are introducing new risks to record-making and recordkeeping for organizations and individuals. Two recent studies explore the impact the online environment and cloud-based services have on digital records creation, use and preservation, focusing specifically on their future use as evidence and social memory.

## Research Question

How do we ensure the trustworthiness (i.e., accuracy, reliability and authenticity) of digital records accessed, shared and stored through social media platforms and service providers utilizing cloud-computing infrastructure?

## Research Projects

In 2012, the **Law of Evidence in the Digital Environment (LEDE) Project** began exploring the challenges presented by digital materials to the law of evidence as it exists. The LEDE Project is a 3-year collaboration between the Faculty of Law and the iSchool at the University of British Columbia, Canada.

In 2013, the **InterPARES Trust (ITrust) Project** began exploring issues of trust regarding digital records in the online environment. ITrust is a 5-year multi-national, interdisciplinary project directed by Dr. Luciana Duranti, based at the Centre for the International Study of Contemporary Records and Archives at the University of British Columbia, Canada.

## Research Methodology

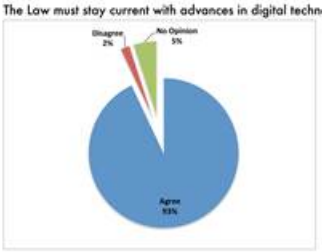
An extensive LITERATURE REVIEW in the legal and archival domains for concepts and issues of trustworthiness, digital records, digital evidence, and social media contracts was conducted. Followed by a review of case law in North America pertaining to the use of social media content in civil and criminal cases, specifically the issue of authentication.

A qualitative SURVEY of professionals involved with digital evidence in legal proceedings was conducted, followed by in-depth INTERVIEWS with selected survey participants.

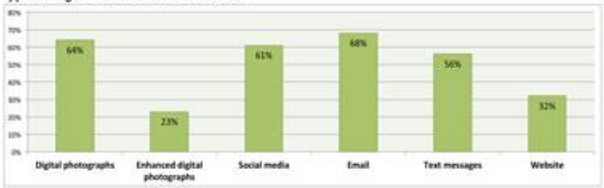
In the context of records management and recordkeeping standards, TEXTUAL ANALYSIS of boilerplate cloud-service contracts from selected providers' Terms and Conditions Agreements, was conducted, including their Terms of Service, Terms of Use, and Privacy Policy.

## Key Survey Findings

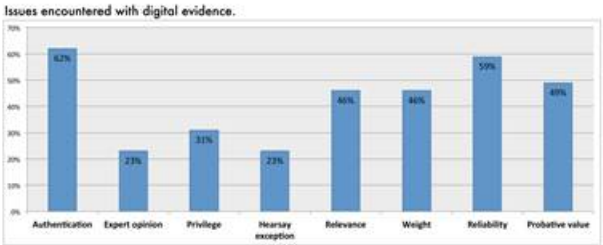
The Law must stay current with advances in digital technology.




Types of digital evidence that raised issues.




Issues encountered with digital evidence.




**Acknowledgements** This research is supported by a Social Sciences and Humanities Research Council of Canada (SSHRC) Parntership Grant and Insight Grant.

Bushey, J., M. Demoulin, and R. McLelland. "Cloud Service Contracts: An Issue of Trust." *Canadian Journal of Information and Library Science* 39, no.2 (2015): 128-153.

## Key Findings of Cloud-Service Contract Analysis

### Data Ownership

Archivists need to establish whether the party that stores their information and records in the cloud retains ownership. Digital ownership is not necessarily the same as ownership over information transcribed onto a physical medium (*Oxford v. Moss*, [1979] 68 Cr. App. R. 183). Records stored in electronic systems require arrangements that distinguish between the ownership of the records and the storage of the records (ISO 15489-1: 2001, s.8.3.4).

Boilerplate cloud-service contracts assign ownership of user-generated content to the creator, but not the metadata produced during upload, mangement, migration and storage - this is owned by the service provider.

Social media contracts assign ownership of user-generated content to the creator, but retain an unlimited, royalty-free, non-exclusive license to re-use members' content, even after the account has been terminated.

### Availability, Retrieval and Use

One of the drivers for adopting cloud-based services is to have information and records immediately available to an organization to fulfill their current and future business needs. Retrieval in a timely manner is required by FOIPOP laws.

Cloud-service providers promise 99.9% uptime; however this amounts to 9 hours of down-time over a year. In reality a number of major disruptions and data breaches to cloud-based services are reported each year (e.g., iCloud 2014, MySpace rebranding).


### Data Storage and Preservation

Recordkeeping standards state that systems for storing digital records should ensure that the records held within the system remain accessible, authentic, reliable and useable throughout any changes made to the system (ISO 15489-1:2001, s.9.6). Additionally, migrations and emulations conducted by the systems provider should not impact the reliability and authenticity of the records (ISO 15489-1:2001, s.8.3.5).

Cloud-service contracts DO NOT address preservation activities. Backup procedures for user-generated content are the responsibility of the creator (or organization that uploaded the content).

Social media contracts state that the service supports sharing, not storage.

### Data Retention and Disposition

Records management and preservation activities rely on record retention and disposition schedules to perform information governance. Schedules must remain compliant with increasingly complex legal and regulatory environments. Recordkeeping standards suggest that the retention and disposition of records should be implemented and carried out by the digital system in which the records are held (ISO 15489-1:2001, s.8.3.7).

Boilerplate cloud-service contracts and social media contracts DO NOT address data or record retention or disposition.

### Security, Confidentiality and Privacy

Managed access to information and records held in systems ensures the authenticity of the records. Recordkeeping standards require that audit trails and access logs demonstrate that records are being protected from unauthorized access, use, alteration, or destruction (ISO 15489-1:2001, s. 8.3.6). Security measures are demanded by data protection legislation (PIPEDA), as well as sectorial regulations related to financial markets (Sarbanes-Oxley Act and Basel Accords).

Cloud-service contracts focus mainly on the security of physical infrastructure. Cloud-service contracts state that it is the responsibility of the customer to manage access restrictions for their accounts and stored content.

Social media contracts give members a false sense of privacy by providing levels of access control. Criminal and civil cases reveal that content held in social media accounts is discoverable and admissible

### Data Location & Cross-border Data Flows

Cloud computing relies on the processing and storage of data in servers located across the globe. Customer data may be processed and stored in different locations and unknown jurisdictions. Legal concerns arise when customer data is subject to foreign laws and access by foreign agencies (e.g., PATRIOT Act). The law is unclear if a customer's content is tied to the location of the customer, the location of the server, or the location of legal registration of the cloud -service provider (*Microsoft v. United States of America*, 14-2985-cv).

Cloud-service contracts state that control over data location and flow is a fee-based service.

### End of Service

Prior to termination of service all records and associated metadata should be transferred out of the service in a manner that does not impact their reliability, authenticity and useability (ISO 15489-1:2001, s.8.5).

Cloud-service providers may end the service for breach of contract and/or inactivity of the account. Notification of the customer is not required.

In the case of death, social media contracts freeze access to the account and its contents.