Competition: *SSHRC Knowledge Synthesis Grants on the Digital Economy*

Project Title: *The Canadian legal framework for evidence and the Digital Economy: a disjunction?*

Principal Investigator: Anthony F. Sheppard, Professor of Law, UBC
Co-Investigator: Dr. Luciana Duranti, Professor of Library, Archival and Information Studies, UBC

December 1, 2010

Acknowledgements

This project was made possible by funding from SSHRC.

We could not have completed it without the contributions of the student research assistants of the University of British Columbia.

We especially would like to thank Corinne Rogers, doctoral student in archival science, who arranged and participated in all the interviews, conducted the qualitative analysis of the data, and went to Ottawa to represent our team at the meeting of the Digital Economy program grant holders; and Donald Force, doctoral student in archival science, who participated in interviews and reviewed the case law from an archival standpoint. They both substantially contributed to the analysis of existing literature and to this report.

We also would like to thank Kelly E. Lau, graduate student in archival science; and three J.D. candidates in the Faculty of Law, Brian Carter, Mark Crisp, and Jason Shabestari, who did the reviews, respectively, of archival science and diplomatics literature, and of legal literature.

Thanks to them and to our technical wizards, Randy Preston, who also arranged for and took the minutes of all meetings, and Jean-Pascal Morghese.

The Canadian Legal Framework for Evidence and the Digital Economy – A Disjuncture?

Table of Contents

Acknowledgements **2**

Executive Summary **5**

1. Introduction **7**

1.1 Background 8
1.2 Goal 10
1.3 Research Questions 10
1.4 Methodology 10

2. Findings – Literature and Interview Data **11**

2.1 The Canadian Legal Framework for Evidence 13
The Evidence Acts 13
Rules of Court 15
The Interpretation Acts 15
The Electronic Transactions Acts and Electronic Commerce Acts 15
Case Law 16
Standards as part of the legal framework 16
2.2 Definitions: Setting the Stage 17
Digital vs. Electronic 18
Data – Document – Record 19
2.3 Finding the Evidence: Looking for the Smoking Gun 20
Document or Record 20
E-Discovery 22
Hard drives 23
Metadata 24
Unallocated clusters 24
Random Access Memory (RAM) 25
2.4 Using the evidence: Can we trust it? 26
Authentication 26
Hearsay 27
Best Evidence & System Integrity 28
Computer-generated vs. Computer-stored 29
Legal effect and functional equivalence 32
Legal requirements for writing 33
Search and seizure 33
Are there really any problems? 35

3. Conclusion **35**

Appendix I **37**
Definitions from Rules of Court 37
Appendix II **40**
Definitions from Interpretation Acts 40
Appendix III **42**
Canada's Electronic Transactions Acts 42
Appendix IV **43**
Letter of Request for Interview 43
Appendix V **44**
Interview Protocol and Participants 44
Appendix VI **45**
Interview Questions for Legal Professionals 45
1. Digital records and issues of law 45
2. Treatment of digital records – Authenticity 45
3. Identification (recovery and forensic treatment) 46
4. Collection 47
5. Examination 47
6. Presentation 47
7. Management and Preservation 48
8. Concluding Questions 49
Appendix VII **50**
Selected Codes Used in Analysis of Sources 50
Bibliography **54**

Executive Summary

Laws are intended to regulate human conduct, but law-makers (legislatures, courts, tribunals, etc.) are limited by their knowledge and understanding of the past and current forms of human conduct of which they are aware at the time of making laws. Technological change permits new forms of communication that the law-makers could not possibly have imagined when they made laws.

In former days, judges and legislators could not have anticipated, and did not anticipate that the evidentiary rules and procedures they developed as appropriate to forms of communication and recordkeeping prevailing in their time and place would require adaptation to the pervasive use of the computer and Internet in the Digital Economy.

Digital records are different from traditional paper records in many ways, and these differences have implications for the laws of evidence and related legal procedures. Born digital evidence is vastly more extensive, can be more costly to discover, disclose and recover and more invasive of privacy than traditional forms of evidence. It can be at the same time more volatile and more difficult to destroy, and it is easier to change or replicate in various guises.

This project has investigated, through a synthesis of knowledge from legal scholarship and practice, and from diplomatics and archival theory and best practices, the disjuncture between the statutory and regulatory framework for evidence, and the records now prevalent in the digital economy.

What we have learned:

a) A network of statutes and regulations that have developed over decades spanning rapid and dramatic technological development governs documentary evidence in electronic form.

b) Across Canada, definitions in provisions of the various statutes that relate to proof of transactions in the digital economy require revision to achieve uniformity, and to become or remain technology-neutral.

c) *Terms such as "records," "documents," and "data," within Canadian statutes and rules, have been defined inconsistently, and, as a result, challenge the judicial system's intentions to reduce costs associated with the discovery process and limit the time necessary to conduct legal hearings. Further investigation is necessary to determine whether fault lies with the definitions themselves or it is the ever-changing state of technology that the courts fail to fully grasp.*

d) *The concept of authenticity and the means and need for authentication are little understood.*

e) The traditional best evidence rule has little meaning in the digital environment, but its intent needs to be captured and expressed in rules aiming to achieve functional equivalence.

f) There is no consensus about the application of the hearsay rule and its exceptions to all forms of digital evidence.

g) Functional equivalence between digital and paper transactions can only be attained by expressly providing for it in particular statutes, rather than by exclusive reliance on implicit cross-reference in a separate, self-contained statute such as the Uniform Electronic Commercial Transactions Act.

h) On the whole, Canadian law reform agencies are eager to bring laws up to the digital era but require further research and expertise to inform their recommendations.

Therefore, this report recommends that interdisciplinary research integrating the expertise of legal, archival, diplomatic, forensic, and computer and information theorists be conducted to address the identified disjunction between the Canadian legal framework for evidence and the digital economy, and to develop solutions that can be embedded in new legislative and regulatory texts.

1. Introduction

This study is one of twenty-five studies made possible through a *Knowledge Synthesis Grant on the Digital Economy* from the Social Sciences and Humanities Research Council (SSHRC) of Canada. These studies have been conducted across Canada and each explores a unique facet of Canada's digital economy. The digital economy, growing at an exponential rate as the pace of technological change accelerates, holds the promise of prosperity and progress, but also strains our educational, social and legal infrastructure. Knowledge syntheses bring together expertise from different but compatible disciplines to identify, and ultimately propose solutions to, today's complex social and economic problems.

Legal professionals and scholars have begun to write on the unintended consequences of applying laws developed for a paper-based business environment to the growing digital reality. Case law, however, develops slowly, and for every two steps forward there is often one step back. The assumptions we make about paper records often do not apply to digitized and born digital records, and to records stored in computers or generated by them without direct human intervention, and judges and lawyers are not trained in information technology and, for the most part, are not knowledgeable about it. There is, however, a wealth of research into the nature of digital entities conducted by archival scholars and other information professionals that has direct relevance to the challenges faced by the law concerning documentary evidence and its admissibility at trial. This study has carried out exploratory research into the effects of the increasing use of technology in the conduct of personal affairs and public business and on their consequences when digital material must be considered by the legal system. It synthesizes legal, diplomatics, and archival knowledge, identifying in a systematic way the challenges that are being faced.

The focus of this study is the legislative framework in Canada at the federal, provincial and territorial levels as it influences and is challenged by the digital economy. To understand the challenges and the opportunities requires the co-operation of legal experts, who can interpret the law; information technologists, who understand the power and capacity of technology; and records and information professionals, who have researched the nature, characteristics, attributes and trustworthiness of records in all media and of digital records in particular. Much advanced legal and forensic thinking about the issues under consideration, however, is being conducted elsewhere – in the United States, Great Britain and Australia. Accordingly, a large portion of the literature discussed is perforce from outside our borders. To illustrate our points, we have wherever possible made reference to Canadian case law. In a few instances, case law from other jurisdictions has been referenced.

This report cannot claim to be a comprehensive compendium of all the challenges arising from the consideration of digital materials as evidence at trial. However, we believe that

the main problem areas have been identified, through reading, interviews, and text analysis. Further research will be required to offer comprehensive solutions to these challenges.

1.1 Background

Canada has been a leader in developing the digital economy. Among its many innovations, the Government of Canada can celebrate its role in linking all our schools and libraries to the Internet, and promoting the cross-country deployment of broadband and early uptake of information communication technologies (ICTs).[1] The government recognizes that there is work to be done to maintain, and even regain its advantage as other countries embrace digital technologies, and it has committed to launch a "digital economy strategy" to "drive the adoption of new technology across the economy." The goal is to encourage innovation in research and development and artistic endeavor within a framework of laws "governing intellectual property and copyright."[2]

Digital technology offers many advantages to the transaction of business. Email and other communication technologies can reduce costs and delay, being in some cases instantaneous. Use of the Internet eliminates the need for individuals to transact business with each other in person, and offers the benefit of increased efficiency in their dealings. However, unless protective measures are taken, the fact that the transacting parties are not in each other's physical presence when business is conducted increases the risk of impersonation, fraud and forgery.

The impact of digital technology on our lives, however, extends far beyond the uptake and use of new technologies. It has unintended consequences for the ways in which we govern ourselves and structure our society. The implementation of a national digital architecture is necessarily incremental, and public trust is built over time. Nowhere is this seen more clearly than in the development of legislation and the application of statute and common law in cases involving digital evidence.

Laws are intended to regulate human conduct, but law-makers (legislature, courts, tribunals, etc.) are limited by their knowledge and understanding of the past and current forms of human conduct of which they are aware at the time of making laws. Technological change permits new forms of human conduct that the lawmakers could not possibly have anticipated when they made laws. This is especially true with regard to the effect of technological change on human communication and record making.

---

[1] Industry Canada, "Government of Canada Launches National Consultations on a Digital Economy Strategy," available at http://www.ic.gc.ca/eic/site/ic1.nsf/eng/05531.html.
[2] Industry Canada, "Improving Canada's Digital Advantage: Strategies for Sustainable Prosperity," Consultation Paper on the Digital Economy [2010] Available at http://de-en.gc.ca/consultation-paper/.

Rules of evidence, which regulate proof and procedure in legal proceedings, started to emerge in the 16th century through common law decisions, and developed in the 19th century through legislation. Among the most important of these rules are those related to the pretrial procedures of documentary discovery and disclosure, and the trial rules around hearsay, authentication, best evidence and privilege.

The Canadian Law of Evidence, which governs proof in litigation of facts, is the result of hundreds of years of rule making by courts and legislatures. These rules of evidence govern the admissibility in legal proceedings of proof of facts and transactions. The courts and legislatures that established these rules did so long before the current era of digital communications. Lawmakers of the past made rules of evidence for the forms of communication that they were familiar with, which were either oral or written in a stable, persistent way. In these earlier times, judges and legislators could not have anticipated, and did not anticipate that the evidentiary rules and procedures they developed as appropriate to forms of communication and record-keeping prevailing in their time and place would require adaptation to the pervasive use of the computer and Internet we are experiencing today in the digital economy.

Today, digital communications technologies are far more prevalent than the oral and written modes of communication that were dominant when the rules of evidence were produced. Transactions and other communications may occur through e-mail and over the Internet; financial records are created using spreadsheets and databases; banking records are made though system-to-system transactions; digital photography, digital video and audio recordings have made obsolete previous technologies.

Digital records are different from traditional analogue records in many ways, and these differences have implications for the laws of evidence and related legal procedures.[3] Born digital records are not as constrained as analogue records in the wide variety of different formats in which their contents can displayed. They are vastly more extensive in their volume, quantity and dispersal. As a result, digital records can be far more costly than analogue records to produce for disclosure in litigation. Individuals often use the same computer or other device for a wide variety of business and personal communications, which means that compulsory discovery of digital communications can be far more invasive of privacy than discovery of traditional forms of documentary evidence. Digital records can be more volatile and transitory, and easier to alter or replicate, but more difficult to obliterate.

Digital technology is subject to a rapidly increasing rate of obsolescence and this has implications for the long-term retention, preservation and accessibility of digital material. Although paper and other analogue documents can deteriorate over a long period, well-known and accepted techniques are available to preserve them, but similar techniques for the long-term preservation of digital records have only recently been developed in the course of very complex research projects and, although they are

[3] A clear understanding of the differences between the terms digital, electronic, and analogue are critical and will be addressed later in the report.

being tested in a variety of organizational environments, they certainly have not gained common usage. As a consequence, various international and national organizations promulgate standards for record-making and record-keeping which aim to ensure and protect the reliability and authenticity of digital records over time. Moreover, experts in the disciplines of Archival Science and Diplomatics, which focus on the study of records' trustworthiness and accessibility, have developed theory and methods for maintaining them over time, and issued guidelines for digital records creators and preservers based on the findings of international research projects.

1.2 Goal

The overall impact of the digital economy on modes of legal proof is a widespread uncertainty, and the lack of knowledge about the suitability of existing evidentiary rules and procedures to regulate the admissibility of newer forms of digital evidence as proof of facts and transactions is a significant problem at best. The specific purpose of this knowledge synthesis project is to examine the existing Canadian laws and conventions in the context of existing and developing information and communications technologies, and establish whether these rules and procedures are adequate to the task of regulating proof of facts and transactions in the digital economy.

1.3 Research Questions

To reach this goal, the researchers posed the following research questions:
1. Are the existing rules and procedures consistently ad effectively used to regulate proof of facts and transactions in the digital economy?
2. In what ways is the law challenged by the proliferation of digital materials offered in evidence?
3. What are the consequences for the administration of justice of any inadequacies that may be found?

1.4 Methodology

This qualitative interdisciplinary research drew on theory from Archival Science, Diplomatics and advanced legal reasoning. By accessing legal scholars' knowledge of evidence law and its application, and archival scholars' understanding of the nature of digital objects in general, and digital records in particular, it brought together the results of leading edge international research on digital records, federal and provincial legislation, and judgments and opinions from recent case law. The combination of these knowledge areas allowed for an in-depth analysis of the challenges posed to the

traditions of evidence law by the innovation of new communications and record-making technologies.

The researchers conducted an extensive literature review, which included a survey of Canadian law – legislation, rules of court and Canadian case law, legal commentary, and scholarly literature from the legal and archival disciplines. New data was gathered through the qualitative analysis of interviews conducted over the course of several months with lawyers, judges and legal scholars chosen for their familiarity with the presentation of digital materials in litigation. While the researchers attempted to interview a representative cross section of legal professionals spanning areas of responsibility and technical knowledge, this survey research does not claim to be comprehensive of all views. Several interviewees asked to remain anonymous in the presentation of results. We have respected their wishes.

The resulting interview data and the relevant literature were entered into NVivo8 Qualitative Analysis software and coded in an iterative process to identify trends, issues and challenges. Codes were chosen that identified references to:

- specific characteristics of digital records and requirements for their authenticity, reliability, accuracy and usability;
- examples of the application of admissibility rules to digital material;
- examples of the treatment of digital material submitted in evidence;
- definitions of relevant terms found in legislation and relied upon in litigation.

A full list of codes developed and used are found in the Appendix VII.

The results of coding the literature and interview data were subjected to qualitative content analysis. Our findings are outlined in this report.

2. Findings – Literature and Interview Data

Many of the challenges that legal professionals face today result from the fact that computers create and manage records in fundamentally different ways than traditional paper-based forms of recordkeeping (Lynch and Brenson, 1989). We talk about computer files as if they were the equivalent of paper documents, but even a simple word processing file is saved on a computer in a radically different way than its paper counterpart. This can lead to misunderstandings, inconsistencies and mistakes when considering what digital material may constitute evidence of facts or transactions, how it should be authenticated, accessed, presented and preserved.

Definitions are the underpinning of all legislation. Without consistent definitions that adequately account for the characteristics, attributes, and therefore the effects of items described, the law cannot be applied consistently or fairly. Rules of admissibility are changing because of the nature of digital material. Concepts that have been fundamental to admissibility, such as the concept of hearsay, related exceptions to the hearsay rule,

and the concept of original at the core of the best evidence rule, have been shaken by the fact that digital records are not just like analogue records. Their differences have resulted in surprising consequences for the law.

The law does not stand still, however, and lawmakers have been grappling with legislative reform to address issues arising from new technologies for two decades. This report begins with an outline of the Canadian legal framework for evidence – the laws that identify and regulate documentary evidence and set the context for the interpretation of the myriad forms in which information is presented to the court. These laws have undergone several changes, and new laws have been developed to attempt to address the complexities of evidence in digital form.

Following that, the report examines the records themselves and the systems in which they are created, transmitted and stored. What is considered a record in electronic systems and how are these entities treated by the law? Can the concept of "writing" include electronic communication, and are electronic signatures the equivalent of hand-written signatures? Problems arise from the sheer volume of electronically stored information (ESI), and the typical mix of public and private, business and personal information that exists on most computers. These problems are seen clearly in concerns about privacy and privilege, and in the challenges found in the pre-trial discovery phase of litigation. Each area will be considered individually and illustrated, where possible, by examples from existing case law.

The inconsistencies and deficiencies we found in current law when applied to the complexity of digital materials offered in evidence are categorized into three main areas and their subareas:

- Definitions: setting the stage
    - Digital vs. Electronic
    - Data – Document – Record
- Finding the evidence: looking for the smoking gun
    - Document or Record
    - E-Discovery
    - Hard drives
    - Metadata
    - Unallocated clusters
    - RAM
- Using the evidence: can we trust it?
    - Authentication
    - Hearsay
    - Best Evidence & System Integrity
    - Computer-generated vs. Computer stored
    - Legal effect and functional equivalence
    - Legal requirements for "writing"
    - Search and Seizure

- Are there really any problems?

2.1 The Canadian Legal Framework for Evidence

The handling of evidence in proof of facts and transactions in Canada is governed by the federal, provincial and territorial Evidence Acts, and supported by a web of statutes, regulations, standards, and case law. Evidence, be it testimony, exhibits or documentary material is subject to rules about its admissibility. Documentary evidence has evolved from predominantly paper, to various other analogue media such as magnetic tape, microfilm, and photographs, and now to digital material. Some of this digital material is similar to traditional office documents, but increasingly it is becoming more complex in its presentation, provenance, behavior, and requirements for accessing it, presenting it to the court, and preserving it. Digital evidence may be found in stand alone or networked computers, on social media sites, in cell phones, in various storage devices, in automatic teller machines and digital cameras, to name but a few locations. As documentary evidence has changed its form and the media on which it is found, the law has adapted, albeit slowly. In adapting these rules, and through subsequent reforms, the courts have been careful to strike a balance between providing ease of proof of trustworthy records and avoiding, as much as possible, risks of fraud, forgery and unreliability.

The Evidence Acts

The Uniform Law Conference of Canada (ULCC)[4] comprises representatives of the federal, provincial and territorial governments of Canada and various law reform agencies, and works through committees of experts to develop model legislation on various topics for possible adoption by the Parliament of Canada and by the legislative assemblies of provinces and territories. In 1997, the ULCC adopted in principle the text of a proposed *Uniform Electronic Evidence Act* (*UEEA*), and sought consultation prior to final approval.[5] At the following annual meeting in 1998, the ULCC officially adopted the *UEEA*[6] as a model legislation that proposed reform of the traditional common law evidentiary requirements for proof of authentication and best evidence, on the grounds that, while these rules worked well enough for paper records, they could not deal adequately with electronic ones.[7]

The key sections in the *UEEA*, which was adopted verbatim in the Canada Evidence Act (section 31.1-8) deal with authentication, best evidence and presumption of integrity.

---

[4] Uniform Law Conference of Canada, available at http://www.ulcc.ca (accessed on November 29, 2010).
[5] John Gregory, "Canadian Uniform Electronic Evidence Act," available at http://jya.com/eueea.htm (accessed on May 20, 2010).
[6] *Uniform Electronic Evidence Act*, available at http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2 (accessed on May 20, 2010)
[7] For a discussion of the background to the UEEA, see Ken Chasse, "Electronic Records As Documentary Evidence" (2007) 6 C.J.L.T. 141, available at http://cjlt.dal.ca/vol6_no3 (accessed on May 20, 2010).

Authentication
3. The person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Application of the best evidence rule
4.(1) [In any legal proceeding,] subject to Subsection (2), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

4.(2) [In any legal proceeding,] an electronic record in the form of a print-out that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, is the record for the purposes of the best evidence rule.

Presumption of integrity
5. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]

(a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;

(b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Most Canadian jurisdictions welcomed the *UEEA's* new approach to the admissibility of electronic records. In terms of general acceptance and implementation, it was a great success, and literally became uniform law across Canada, regulating the admissibility of electronic records offered into evidence in all criminal and most civil, quasi-criminal, and administrative proceedings. Regardless, case law suggests otherwise – one would expect that such a radical reform would be frequently cited, but this is not the case.

The ULCC took a minimalist approach to reform, and has not updated its initial provisions to meet the changing demands of technological advances. Whereas the

other jurisdictions did not specifically deal with the best evidence and authentication rules in their broader reforms, the ULCC limited its narrower approach to those two rules. However, the need to keep law current with technological changes, especially in the areas of evidence and procedure, cannot be satisfied by legislation issued at a single point in time, but requires continuous and sustained updating (Moses, 2007).

Rules of Court

The rules of court enacted by Canadian jurisdictions govern civil litigation practices. For purposes of civil discovery of documents, they contain a range of definitions of "documents" or "records," many of which are by now very dated. Several jurisdictions have enacted new rules of court in the past few years that explicitly include reference to digital information. This only further heightens the distinct lack of uniformity in reference to electronic and computer documents.

The Interpretation Acts

Most Canadian jurisdictions have enacted statutes entitled *Interpretation Acts*, which provide rules of interpretation applicable to their enactments and definitions of specific terms not otherwise defined in the enactment concerned. As will be discussed, these definitions are often a source of confusion because they are not adequate to handle the complexity of digital material.

The Electronic Transactions Acts and Electronic Commerce Acts

The ULCC followed adoption of the *UEEA* two years later with the *Uniform Electronic Commerce Act* (*UECA*), proposed as "the model upon which provincial and territorial governments can develop a harmonized approach to electronic commerce" (Davies, 2008). The legislation adopts a functional equivalence approach, looking not at the medium of the documents and records involved, but the function they serve. It purports to "ensure that electronic communications are capable of conveying the kinds of intentions that are necessary to support contractual relations." Part One establishes rules for the functional equivalence between electronic and paper documents, the circumstances in which electronic documents may be used in the transaction of business. Part Two covers specific types of communications, correction of errors, and "deemed or presumed time and place of sending and receiving computer messages" (Davies, 2008).

To date, this model legislation has significantly influenced the federal *Personal Information Protection and Electronic Documents Act* SC 2000, c 5; and most of the provincial/territorial statues. The Northwest Territories completed a consultation period seeking feedback on whether or not to adopt the model *Electronic Commerce Act* in February 2010, but no legislation has resulted so far: online, Consultations, http://www.justice.gov.nt.ca/Consultation/ElectronicCommerceAct.shtml. In 2001, Quebec went its own way with *An Act to establish a legal framework for information technology*, RSQ, c. C-1.1. The list of statutes and their dates of passage can be found in Appendix III.

Case Law

Case law develops as courts interpret statutes and apply precedent to decide the cases before them. Judges have applied a cautious approach to the handling of digital evidence, and the body of Canadian case law developing precedent in this area is small. However, pressure from sheer quantity of digital material entering our court system, and examples from other common law jurisdictions presage change ahead. As one interviewee remarked, "an examination of the case law would lead to the mistaken conclusion that there was no problem, no need for further legislation…"

Even in the absence of legislation and precedent, some judges have expressed a willingness to admit new forms of evidence resulting from advances in technology, as long as their reliability was not disputed and they did not impact either the traditional roles of judge and jury or court processes.[8] However, judges have also expressed a conservative point of view against initiating broad reforms of the common law rules of evidence to meet modern needs and encouraging the legislatures to take on this sort of project.[9] Currently, the Supreme Court of Canada expresses a preference for confining the courts' role to initiating only "incremental" updating of the common law to meet changing times, leaving broader reforms of complex areas to the legislature.[10] Comprehensive and continuing reform of the procedural and evidentiary aspects of digital records is a matter for legislatures, not for the courts.

Standards as part of the legal framework

This does not mean that legal professionals are not addressing these and other concerns of digital evidence. The Sedona Canada (2008), a nonprofit law and policy think tank of legal experts, has already issued two editions of principles to be followed in the production of digital records. These guidelines emphasize that the key to having trustworthy documentary sources is to generate them according to specific authenticity

---

[8] *R. v. Béland*, [1987] 2 S.C.R. 398, 43 D.L.R. (4th) 641 at paragraph 20; *R. v. Nikolovski*, [1996] 3 S.C.R. 1197, 141 D.L.R. (4th) 647.

[9] *Myers v. Director of Public Prosecutions*, [1965] A.C. 1001 (H.L), not followed in *Ares v. Venner*, [1970] S.C.R. 608, 14 D.L.R. (3d) 4.

[10] *R. v. Salituro*, [1991] 3 S.C.R. 654, 1991 CanLII 59 (S.C.C.); *Grant v. Torstar*, [2009] 3 S.C.R. 640, 2009 SCC 61, paragraph 46; in *Watkins v. Olafson*, [1989] 2 S.C.R.750, McLachlin J. (as she then was) for the court said: "Generally speaking, the judiciary is bound to apply the rules of law found in the legislation and in the precedents. Over time, the law in any given area may change; but the process of change is a slow and incremental one, based largely on the mechanism of extending an existing principle to new circumstances. While it may be that some judges are more activist than others, the courts have generally declined to introduce major and far-reaching changes in the rules hitherto accepted as governing the situation before them. There are sound reasons supporting this judicial reluctance to dramatically recast established rules of law. The court may not be in the best position to assess the deficiencies of the existing law, much less problems which may be associated with the changes it might make. The court has before it a single case; major changes in the law should be predicated on a wider view of how the rule will operate in the broad generality of cases. Moreover, the court may not be in a position to appreciate fully the economic and policy issues underlying the choice it is asked to make. Major changes to the law often involve devising subsidiary rules and procedures relevant to their implementation, a task which is better accomplished through consultation between courts and practitioners than by judicial decree. Finally, and perhaps most importantly, there is the long-established principle that in a constitutional democracy it is the legislature, as the elected branch of government, which should assume the major responsibility for law reform."

requirements and maintain them in the correct way throughout their existence; unbeknownst the legal community, records professionals (i.e., archivists and records managers) have been making such an argument for the past twenty years (Duranti and MacNeil, 1996; Hedstrom, 1997; Bantin, 2002).

The judiciary has tried to address the problem by specifying minimum requirements for admissible digital evidence and by providing guidelines for meeting these requirements, but has not provided guidelines for assessing material that does not obviously correspond to the requirements (British Columbia Electronic Evidence Project, 2006; Guidelines for the Discovery of Electronic Documents, 2005, Supreme Court of B.C., 2006). Computer Forensics has also tried to provide guidance, but it does not focus on the documentary evidence *per se*, but on the environment of its creation and maintenance, regardless of the efforts made by scholars in the field to find appropriate methods to assess the digital entities themselves (Casey, 2007; Carrier, 2003; Pollitt and Shenoi, 2005).

Standards developing bodies, like the Canadian General Standards Board, have attempted to address these needs by issuing requirements based on archival concepts (Government of Canada, 2005), and scholarly archival literature on the subject has pointed out the pitfalls of leaving such responsibility to legislators rather than to researchers (Iacovino, 2006; Cox, 2006). Thus, it is essential that proposed changes to the law of evidence result from an interdisciplinary approach based on the convergence of knowledge from a variety of disciplines: law, diplomatics, archival science, computer forensics, cyber-security, quality assurance and forensic readiness.

What we have learned: *A network of statutes and regulations that have developed over decades spanning rapid and dramatic technological development governs documentary evidence in electronic form.*

2.2 Definitions: Setting the Stage

The interpretation of laws depends on the interpretation of the definitions they contain. Clear definitions enhance understanding and usability; poor definitions lead to misunderstanding and challenge. The digital economy is dependent on clarity of terms such as electronic and digital record, data message, information system, and electronic and digital records system, as one would expect. But the digital economy exists within a framework of laws drafted before digital technology, and so is also bound by the definitions that precede that technology. We have an intuitive understanding of terms like document, record, writing, and signature. Their statutory definitions reflect and codify these assumptions. However, these definitions now reveal ambiguities, unintended at the time of their drafting, which may have negative consequences when trying to handle digital material. Statutory definitions for these and related terms are frequently confusing and sometimes contradictory. This affects the interpretation of evidence and the establishment of proof of facts and transactions.

Digital vs. Electronic

To lay a solid foundation, the usage of the terms "electronic" and "digital" must first be clarified. Definitions found in legislation refer consistently to electronic entities – records, documents, data, signatures and so on, but common parlance conflates "electronic" and "digital." Understanding the difference between electronic and digital entities may have consequences for the interpretation of potential evidence. To confuse matters further, the fact that ESI (electronic documents, electronic records, electronic data) may be either analogue or digital in representation is implicit in legal definitions but never explicitly stated.

Research into the nature of digital records brings some clarity to this problem. The InterPARES project, a twelve-year, three-stage international research endeavour supported by funding from SSHRC, offers definitions from its glossaries that are specific to the information professions.[11] The InterPARES 2 Glossary offers the following definitions for electronic, analogue and digital:[12]

> **Electronic** – Device or technology associated with or employing low voltage current and solid state integrated circuits or components, usually for transmission and/or processing of analogue or digital data.
>
> **Analogue** – The representation of an object or physical process through the use of continuously variable electronic signals or mechanical patterns.
>
> **Digital** – The representation of an object or physical process through discrete, binary values.

The fact that electronic objects (records, documents, etc.) may be either analogue or digital becomes an important factor in reading and interpreting legal definitions. An electronic object is one that is transmitted and rendered by electronic equipment. Whether that object is analogue or digital is determined by its manner of encoding.

The *Electronic Commerce Act of Ontario* (S.O. 2000, Ch. 17, s. 1) defines "electronic" broadly: "'electronic': includes created, recorded, transmitted or stored in digital form

---

[11] The InterPARES Project (International Research on Permanent Authentic Records in Electronic Systems) began in 1999 to develop knowledge about digital entities so that authentic digital records could be created, maintained and preserved over that long term. This knowledge is being used to guide policy development and digital records management so that creators and users can be confident that the digital records on which they rely are trustworthy – authentic and reliable. The project has run in three phases. InterPARES 1 ran from 1999 – 2001 and researched the preservation of digital records – both born digital and digitized – in databases and document management systems. InterPARES 2 (2002 – 2007) explored reliability and accuracy of experiential and dynamic records in complex systems during their entire lifecycle, from creation to permanent preservation. It focused on records creation and preservation in the artistic, scientific and government sectors. InterPARES 3 (2007-2012), currently involving teams from 15 different countries, puts theory into practice, working with small and medium-sized archives and organizations through a variety of individual case studies and general studies.

[12] InterPARES 2 Glossary, www.interpares.org, current to November 26, 2010.

or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means and "electronically" has a corresponding meaning; ("électronique", "par voie électronique")." The definition in the *Land Title Act* of British Columbia (R.S.B.C. 1996, c. 250) is similar, if slightly simpler: "'electronic' includes created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic or optical means or by any other similar means."

These definitions are not particularly problematic, even if they are somewhat imprecise. A simpler definition, which is closer to that commonly used by information and computer technology professions, is found in the American *Uniform Electronic Transactions Act* (1999): "'Electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."[13]

Data – Document – Record

Difficulties begin to arise in the definitions of various electronic objects. Overlapping and inconsistency occur in the definitions and their interpretation of "data," "information," "document," and "record." Consider, for example, the following. In the *Canada Evidence Act*, electronic records provisions (R.S. 1985, c. C-5, s. 31.8), "data" means "representation of information or of concepts, in any form." In the same section, "electronic document" is defined as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data." In the same Act, s. 30.1 determines the admissibility of business records (the business records exception to the hearsay rule) and in s. 30.12, "record" is defined as "the whole or any part of any book, document, paper, card, tape or other thing on or in which information is written, recorded, stored or reproduced…" Two further clauses inject the possibility of confusion when one party adduces digital material as evidence. Section 30.1 states: "Where oral evidence in respect of a matter would be admissible in a legal proceeding, a record made in the usual and ordinary course of business that contains information in respect of that matter is admissible in evidence under this section in the legal proceeding on production of the record." Section 30.10 (a)(i) renders inadmissible "such part of any record as is proved to be (i) a record made in the course of an investigation or inquiry."

A recent example of a challenge – unsuccessful though it was – to the admissibility of electronic records based on these points can be found in *R. v. L.B.*, 2009 BCSC 1194. In the ruling on admissibility of an electronic document, the Honourable Madam Justice H. Holmes refuted the argument of counsel for the accused. The document in question was produced from electronic data created and stored in an electronic records system

[13] This Act, was proposed by the National Conference of the Commissioners of Uniform State Laws in 1999, and has since been adopted by 48 states and provinces (i.e., District of Columbia, U.S. Virgin Islands, and Puerto Rico). The full version of the Act may be found online at http://www.law.upenn.edu/bll/archives/ulc/uecicta/eta1299.htm (accessed 29 November 2010).

of a business as part of the functioning of that business. The document was required by a production order to be produced for the purposes of trial. Counsel for the accused argued that it was inadmissible because it was produced as part of an investigation, however the learned judge determined that the data underlying the document pre-existed the production order. In making her argument, the learned judge invoked the definitions of "data," "electronic document," and "record." The usefulness of these definitions may be questioned when one reads such statements as "The definition makes no express reference to electronic documents, but may clearly include them…" (at paragraph 10) and "Exhibit A is an 'electronic document' presenting data (which themselves are also an "electronic document") recorded or stored as part of … business records…" (at paragraph 11). Thus in this case, data is an electronic document, which is a business record.

Returning to the InterPARES glossaries, we find definitions of data, document, and record (as well as digital data, digital document and digital record) based on their respective attributes rather than on medium or form. Each definition builds on the previous one.

> **Data** – The smallest meaningful units of information [where information is an assemblage of data intended for communication either through space or across time].
> ***Digital data*** *– The smallest meaningful units of information, expressed as binary bits that are digitally encoded and affixed to a digital medium.*
>
> **Document** – An indivisible unit of information [which is made up of data] constituted by a message affixed to a medium (recorded) in a stable syntactic manner. [Accordingly,] A document has fixed form and stable content.
> ***Digital document*** *– A digital component, or group of digital components, that is saved and is treated and managed as a document. See also: analogue document.*
>
> **Record** – A document made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference.
> ***Digital record*** *– A digital document that is treated and managed as a record.*

What we have learned: *Across Canada, definitions in provisions of the various statutes and regulations that relate to proof of transactions in the digital economy require revision to achieve uniformity, and to become or remain technology-neutral.*

2.3 Finding the Evidence: Looking for the Smoking Gun

Document or Record

For purposes of civil discovery of documents, the rules of court enacted by Canadian jurisdictions contain a range of definitions of "documents" or "records" (see Appendix II for a complete list). For example, the British Columbia Supreme Court Civil Rules

(B.C. Reg. 168/2009) define a document as having "an extended meaning and includes a photograph, film, recording of sound, any record of a permanent or semi-permanent character and any information recorded or stored by means of any device." Ontario's Rules of Civil Procedure (R.R.O. 1990, Reg. 194) contain a slightly narrower definition citing a document as "a sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account, and data and information in electronic form." Alberta's *Rules of Court* (Alta. Reg. 124/2010, appendix) do not contain a definition for a document but define a "record" as "the representation of or a record of any information, data or other thing that is or is capable of being represented or reproduced visually or by sound, or both." Finally, Nova Scotia's Rules of Civil Procedure (2008) distinguish "document" from "electronic information." These Rules define the former as "a document that is not electronic information, including a print version of electronic information and a non-digital sound recording, video recording, photograph, film, plan, chart, graph, or record" and the latter as a "digital record that is perceived with the assistance of a computer as a text, spreadsheet, image, sound, or other intelligible thing and it includes metadata associated with the record and a record produced by a computer processing data." Overall, there is a distinct lack of uniformity in reference to electronic and computer documents. Some of the earlier definitions are very dated, whereas the more recent definitions in the Ontario and Nova Scotia rules of court explicitly include digital information. Here again, however, we see a lack of consistency in the use of "electronic" and "digital."

Federal, provincial and territorial jurisdictions, with the exception of Ontario, have enacted statutes, entitled *Interpretation Acts,* which provide rules of interpretation applicable to their enactments and definitions of specific terms (see Appendix III). These definitions apply to the words contained in their enactments in the absence of more specific definitions in the enactment concerned. All the definitions omit any reference to "digital" or "electronic." The definitions only refer to information "recorded or stored," which is unduly restrictive of the various modes of communication using current or future technology. Another concern is that some definitions refer only to "words" rather than to information more generally. Perhaps use of the term "includes" may permit an expansive interpretation of these definitions, but with further research, more inclusive explicit definitions could be developed.

In our interviews with legal professionals, the following exchange, paraphrased, reflected the general attitude towards records:[14]

> Researcher*: So, what do you consider to be digital records?*
>
> Interviewee*: Anything that you can find on digital media.*

[14] Paraphrased and generalized interviewee responses are included in this report, in italics and not attributed to individual interviewees. All interviews were conducted by student research assistants in accordance with the requirements of the Inter-Agency Advisory Panel on Research Ethics, Tri Council Policy Statement, Ethical Conduct for Research Involving Humans. See Appendix V for the complete list of interview questions.

This all-encompassing perspective is an alarming trend among the courts, especially as judges rule whether certain types of ESI constitute documents or records for discovery and admissibility purposes.

E-Discovery

During the past several years, the discovery process has received a significant amount of attention from legal scholars and there have been several recent publications offering overviews of the various legal issues that arise with it (Burke et al., 2008; Hrycko, 2010; Finlay, Vermette, and Statham, 2010). This pre-trial phase of litigation involves parties identifying, collecting, preserving, and exchanging documentation. Discovery plays a vital role in litigation, often determining whether the case proceeds to trial, ends in a settlement, or is withdrawn due to a lack of information. More importantly, in *R. v. Stinchcombe*, [1991] 3 SCR 326, Canada's Supreme Court ruled that full disclosure is necessary for judicial fairness and advances the search for truth. Yet, in the digital age, electronic discovery (e-discovery), or simply the discovery process involving ESI, is more complicated for several reasons, including the sheer volume of information and its dispersal throughout an organization, its persistent quality (i.e., pressing the delete key does not completely remove a document from a computer system) and its dynamic (i.e. easy to duplicate, move, and manipulate) nature (Shillling, 2006; Murray, Chorvat, and Bell, 2008). As a result, the legal system has experienced an increasing number of prolonged legal battles and, with them, an abrupt rise in litigation costs. In some instances, the parties have been known to debate whether certain ESI falls within the jurisdiction's definition of either a document or record, with the implication that, if it does not meet the requirements, then the information does not need to be disclosed.

Inconsistencies with terminology and definitions contribute to the growing problems associated with the discovery process. Even the most fundamental concept, such as that of digital document, has proven difficult for the courts. In 2009, the Toronto Police questioned whether the *Municipal Freedom of Information and Protection of Privacy Act* (R.S.O. 1990, c. M. 56) required them to fulfill a public records request which, to be met, required them to generate records from existing computer hardware which contained new software and a algorithm that they did not use in their normal and ordinary course of business.[15] At issue was the concept of "record." The Police argued that, because the request required the use of new software, the information being sought did not constitute a "record" under s. 2(1)(b) of the Act, which defines a record to mean:

> any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
>
> (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary

[15] *Toronto Police Services Board v. (Ontario) Information and Privacy Commissioner*, 2009 ONCA 20.

> material, regardless of physical form or characteristics, and any copy thereof, and
>
> (b) subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

Initially, the Adjudicator rejected the Police's argument saying the information being requested was a record, but the Divisional Court disagreed, claiming it was not a record. The Court of Appeal overturned this "narrow interpretation" saying the lower court's decision meant that "access would be determined based upon the coincidence of whether the software was already in use, regardless of how easy or inexpensive it would be to develop" (at paragraph 57). According to the Court of Appeal, the information produced from the new software fell within the definition of a record and needed to be produced in accordance with the Act. Other courts have addressed seemingly more complicated matters of ESI, such as determining whether hard drives, metadata, unallocated clusters, and random access memory (RAM) and these rulings have produced mixed results, and indicate there is no clear consensus for what is or is not a document or record.

Hard drives

In 2006, the Honourable Justice E. Myers of the British Columbia Supreme Court stated, "[i]t is true that documents contained in electronic form present new challenges. That does not mean, however, that the Court should lose sight of the underlying principles regarding document production."[16] In *Desgange v. Yeun*, he ruled that the plaintiff did not have to disclose her hard drive to the defendant because the documents in question:

> stand in no different light than paper documents, and the hard drive is the digital equivalent to a filing cabinet or document repository. A request to be able to search a party's filing cabinets in the hopes that there might be found a document in which an admission against interest is made would clearly not be allowed. Its digital equivalent should also not be allowed."[17]

Yet, two years later, in *Chadwick v. Canada (Attorney General)*, 2008 BCSC 851, he ordered the disclosure of the defendant's personal computer, including its hard drive. In this ruling, Justice Myers acknowledged his 2006 decision but said that "the analogy of a hard drive to a filing cabinet may only be taken so far" because it is a "loose" analogy. The difference between the two cases being that *Chadwick* involved the recovery of deleted files, a process which requires a records forensic expert to examine the contents of the entire hard drive. Despite the rationale for ordering the

[16] *Desgange v. Yeun*, 2006 BCSC 955 (CanLII) at paragraph 20.
[17] Ibid.

disclosure in one case but not the other, these two decisions show that, when attempting to analogize new technology with traditional paper-based concepts, the analogies often are inadequate and result in inconsistent legal rulings.

Metadata

Metadata is another concept which the courts have had difficulty in describing and defining by drawing an analogy to paper documentation. In *Desgange v. Yeun*, Honourable Justice E. Myers ruled that metadata met the definition of a "document" per the Supreme Court Rules of Court. He articulated that metadata, while different from analogue and paper records, is "'information recorded or stored by means of a device' and therefore meets the definition of a document defined by the Rules." A year later, Master Sproat of the Ontario Superior Court of Justice described metadata by drawing the following analogy: "In my view, the metadata is akin to a "time/date stamp" affixed to a letter or the "fax header" that indicated the time/date of faxing and receipt."[18] More recent judicial attempts to define metadata have improved upon that early pronouncement but still reveal contradictory views about its characteristics. For example, a judicial definition stated as follows: "Metadata is a report of recorded data that is generated by computer software. It is not something created by the user; rather it is based on what the user does with their computer."[19] From this definition, it might be inferred that human cannot interfere or tamper with metadata. Yet, Master D.E. Short in *Warman v. National Post Company*, 2010 ONSC 3670, 2010 OJ No 3455 (QL) correctly acknowledged that, although metadata is not generally visible, it is capable of being falsified.

Unallocated clusters

Unallocated clusters are deleted data residing in a computer's hard drive. When a person creates a Word document, the computer creates a space on the hard drive for the corresponding file and, as long as that file is being used, the space is called an allocated cluster. When the user deletes the document, the machine does not automatically reuse the space; instead, it turns the space into an inactive file, or unallocated cluster, which the operating system does not acknowledge during its normal activity. While the deleted information may be retrieved, it has been stripped of all its contextual information, and this makes specific identification of deleted files an economically unsound reality.[20] Despite this fact, in 2008, Justice Elliot Myers of the British Columbia Supreme Court ruled that the unallocated clusters of a plaintiff's hard drive had to be searched by the defendant's legal team. In *Honour v. Canada (Attorney General)*, 2008 BCSC 1631, he does not explicitly define unallocated clusters as a "document" per the British Columbia Supreme Court Rules, but he implies that these deleted files are, in fact, documents when he explains that his "rationale for the forensic analysis of the hard drive is to ensure that all relevant documents are produced. Therefore, if a document or partial document is retrieved from an

---

[18] *Hummingbird v. Mustafa*, 2007 CanLII 39610, OJ No. 3624 (QL) at paragraph 9.
[19] *Bishop v. Minichiello*, 2009 BCSC 358 (CanLII), at paragraph 50, 94 B.C.L.R. (4th) 170.
[20] Computer Forensics International, "Evidence Recovery: How Hard Drives Work." Available online at http://www.cf-intl.com/evidence_recovery_basics.htm (last accessed 29 November 2010).

unallocated cluster, and it is relevant, I would expect it to be produced even though it is unable to be dated" (at paragraph 14). Furthermore, even when certain files are produced, there are authentication issues associated with the data because, due to the lack of contextual information or some of the files' metadata, it becomes difficult to determine the trustworthiness and authenticity of the files. As one interviewee explained: "You might be able to tell by context there, but you are not going to be able to say 'yeah, this guy created it' or 'yeah, this guy saw that.' You really have no idea how it got on there a lot of the time."

Random Access Memory (RAM)

RAM is a type of computer storage on which an individual's computer relies randomly to operate all the different software and programs. One of the underlying features of RAM is that it is constantly in use while the computer is running but is considered volatile memory, that is, the information stored in this area is typically lost when the machine is turned off. While no Canadian judge has had to rule on RAM,[21] case law from the United States indicates that it may be a problematic type of ESI for judges and litigations alike. In *Columbia Pictures Industry v. Bunnell et al.*, 2007 U.S. Dist. LEXIS 46364 (C.D. Ca, May 29, 2007), Magistrate Jacqueline Chooljian's ruled that the RAM of the defendant's computers be preserved and disclosed. The Magistrate relied primarily on the fact that other courts had defined RAM as a document and allowed for its discoverability; she saw no reason to break this precedent. These previous rulings stated that RAM is discoverable because it is "temporary storage," or is "fixed" at one point in time to a tangible medium. Upholding the Magistrate's decision, Judge Florence-Marie Cooper of the District Court of the Central District of California, stated that the defendants' "argument that RAM holds data for such a short duration that it is not stored subject to later access and retrieval simply has no merit."[22] While there has been some consensus that this type of ESI is a document per the Federal Rules of Civil Procedure, case law indicates the court's persistent reliance on the notion of fixity without forethought to the financial implications or practicality of the order; such rulings may increase the costs associated with the discovery process and prolong litigation battles.

***What have we learned*:** *Terms such as "records," "documents," and "data," within Canadian statutes and rules, have been defined inconsistently, and, as a result, challenge the judicial system's intentions to reduce costs associated with the discovery process and limit the time necessary to conduct legal hearings. Further investigation is necessary to determine whether fault lies with the definitions themselves or it is the ever-changing state of technology that the courts fail to fully grasp.*

---

[21] The closest the Canadian courts have come to address the disclosure of the RAM is when breath samples were taken and analyzed via an Intoxilyzer device, for example see *R. v. Murray*, 2010 ONCJ 151; *R. v. Duff*, 2010 ABPC 250; and *R. v. Kazmer*, 2009 ONCJ 506. It is unclear how closely this device resembles that of the typical laptop or desktop computer and its RAM.

[22] *Columbia Pictures Industry v. Bunnell et al.*, 2007 U.S. Dist. (C.D. Ca. August 24, 2007) LEXIS 63620 (QL) at **11, 245 F.R.D. 443.

2.4 Using the evidence: Can we trust it?

The Canadian approach to electronic material offered into evidence at trial is that it is to be treated as documentary evidence (Mason, 2010). However, Canada has a low threshold of admissibility, which is not compatible with the complex nature of digital records and electronic records systems (Chasse, 2010).

Records offered as evidence at trial are subject to traditional admissibility rules – the authentication rule, best evidence rule, and the hearsay rule and its exceptions, most commonly the business records provisions. Digital records are also governed by the electronic evidence provisions.

Authentication

> Researcher*: Do you make a distinction between what is a record and what's not a record? And do you treat them the same way?*
>
> Interviewee*: I'm not sure that 'record' in the abstract has any legal meaning. You are either admitting a document or admitting a record because it's authentic.*

According to the traditional rules for admissibility of documentary evidence, documents proffered as evidence must be authentic, that is, they must be what they purport to be. Currently, in North America, when introducing records to be admitted as evidence, the proponent, that is, the one introducing the records, is responsible for establishing a foundation of reliability. While this may be done in a number of different ways, typically the onus falls on the opponent to challenge the trustworthiness of the evidence and raise a reasonable doubt that the evidence is not what it purports to be. Some legal professionals have questioned whether it is feasible for the opponent to raise a reasonable doubt about the authenticity of the evidence, because it may be difficult to gain access to the system that generated the information and determine whether, in fact, it was operating properly at the time the evidence was generated. They advocate the need for a shift in the focus of these admissibility rules (Peritz, 1986; Gahtan, 1999; Arkfeld, 2006; Buskirk and Liu, 2006; Paul, 2004 and 2008). The current statutes and rules of evidence have led one legal scholar to argue that there is an "authenticity crisis" (Paul, 2008), while another author contends that the judicial system may not be experiencing so much an authenticity crisis as a reliability crisis (Parry, 2009).

The following interview excerpts illuminate the challenges posed by digital records to the traditional concepts of hearsay and best evidence, and the variety of responses from legal professionals.

> Researcher*: What, for you, are the characteristics of an authentic digital record?*
>
> Interviewee*: A lot of it is context. You can tell just by looking at it whether it's authentic.*

In response to a question about determining authenticity of proffered evidence, one interviewee replied, "Authenticity's virtually almost a given – if it's seized from a suspect's computer, or produced from an institution under a production order or what have you, the authenticity's very rarely an issue."

Ken Chasse admits that the authentication rule is "a minor player in Canada," requiring proof of authorship and authority to publish a statement as that of the author. It is rarely raised as an objection in regard to admissibility. He states that in his forty years as a practicing criminal lawyer, he never had to research the authentication rule for any case. He suggests, however, that this is not as it should be and that the authentication rule should have more prominence, serving, for electronic evidence, in place of the obsolete best evidence rule.

What we have learned: *The concept of authenticity and the means and need for authentication are little understood.*

Hearsay

> Researcher: *Can you talk a bit about what you think are the challenges to digital material in legal proceedings with respect to admissibility?*
>
> Interviewee: *I would think that some of the challenges would be the creation, proving the creation, and authenticating them.*
>
> Researcher: *Can you expand on what the specific challenges to authentication would be with regards to electronic records.*
>
> Interviewee: *I think it would be a matter of proving that it's made in the ordinary course [of business] and what the procedures are to create that evidence.*

Documentary evidence is generally considered to be hearsay, that is, a human statement made outside court and accepted for the truth of its contents, and therefore inadmissible, unless it is acceptable through an exception to the hearsay rule. The most important exception is the business records exception, which states that a record created in the usual and ordinary course of business can be presumed to be authentic and reliable, and is therefore as trustworthy as oral evidence, and so admissible. Section 30.1 of the *Canada Evidence Act* states: "Where oral evidence in respect of a matter would be admissible in a legal proceeding, a record made in the usual and ordinary course of business that contains information in respect of that matter is admissible in evidence under this section in the legal proceeding on production of the record."

The definition of what may be considered a record in the eyes of the court has already been discussed. But are all electronic (digital) records to be considered hearsay? In the course of the interviews conducted, there was no agreement on this matter.

That there are deficiencies in the rules of admissibility contained in the Act is evidenced by the absence of case law referring to it. In our view, judges and lawyers are insufficiently knowledgeable about the Act, about the applicability of the hearsay rule to computer records, or about computers' unreliability and its impact in assessing weight. Divergence in the rules of admissibility across Canada, lack of cases, and preference for the traditional common law rules of admissibility over the statutory ones in the courts indicate the Act is doing little to add certainty to the law (Duranti, Rogers, and Sheppard, 2010).

According to Chasse, traditional business records hearsay rule exceptions give a false sense of security about the accuracy of digital records. It is a common assumption that people become more accurate by carrying out the same activity repeatedly. Therefore the activity repeated within the "usual and ordinary course of business," and "the regularly conducted business activity," are assumed to be adequate guarantees of accuracy. But computer accuracy does not improve with repetition alone. Humans trained in "habits of precision" become more accurate. But computers, if programmed or operated incorrectly, will always be wrong no matter the amount of repetition.[23]

Best Evidence & System Integrity

Documentary evidence must adhere to the best evidence rule, that is, it must be original, unless the original document/record is unavailable. Digital entities pose a challenge for this traditional rule. Research has shown that the concept of original is meaningless in the digital environment, although one can speak of records having "the force of originals" (Paul, 2008). When the best evidence rule gained the force of law, it was to minimize the risk of admitting unreliable and inaccurate records resulting from hand copying. However, all digital duplicates are, or appear to be identical (their metadata might be different). Reliability in the digital environment comes not from the record itself but from the integrity of the system which generates and stores it and from the controls exercised on the creation, maintenance and use of the record in such system. The electronic evidence provisions were drafted by the Uniform Law Conference of Canada in 1998 to address this issue. The resulting *UEEA* which, as mentioned earlier, was incorporated into the *Canada Evidence Act* (s. 31), and many of the provincial and territorial acts, established that: (1) authentication is of the computer system, not the record; (2) the best evidence rule is abolished; (3) no discussion is needed of the hearsay rule or its exceptions for computer records; (4) no discussion of weight is needed.

The electronic records provisions of the federal, provincial and territorial evidence acts, adapted from the *UEEA*, stipulate that systems integrity be the standard by which the best evidence rule is superseded for digital evidence. However, a showing of systems integrity lays a foundation for the accuracy presumed from the "usual and

[23] Chasse, DEP interview

ordinary course of business," namely the business records exception to the hearsay rule.

What we have learned: *The traditional best evidence rule has little meaning in the digital environment, but its intent needs to be captured and expressed in rules aiming to achieve functional equivalence.*

Computer-generated vs. Computer-stored

The confusion over computer technology within the legal system is never more apparent than when considering the difference between computer-generated and computer-stored records. The former, computer-generated records, are products of an electronic process, resulting from the computer making a decision without human intervention (e.g., an ATM receipt). The latter, computer-stored records, are records created by a person, saved, and maintained in a computer system (e.g., a Word or Excel file) (Paul, 2008). Not surprisingly, the distinction is often not black and white. For example, a digital record may be a human statement stored in a computer but it will also contain computer-generated information embedded in it—the record's metadata.

There has been little discussion in Canada distinguishing computer-stored from computer-generated records.[24] While only a limited number of Canadian cases have referred to "computer-stored" information, only one of them, *University of Regina v. Pettick*, implicitly distinguishes the terms.[25] In this case, Justice Macleod wrote:

> The field of computer law is relatively new, and most commentaries refer to computer records taken from computer stored information as distinct from engineering simulations and information generated by the computer. Where plots or plans and information generated from engineering raw data, accurately fed into a computer operating under a theoretically sound and technically accurate program, are offered to the court, I would expect that a greater evidentiary foundation would be required than for computer records.[26]

The case involved computer-generated simulations (i.e., computer-generated information) and the witness called to authenticate the evidence. At issue was whether the witness had enough expertise with the computer's software and procedures to render the foundation evidence he provided reliable, but in this situation, the witness was not responsible for the design of the program used to generate the simulations. Though Justice Macleod referenced two publications stating that a lay witness may authenticate *computer-stored* data, both references emphasized

[24] The distinction between these two types of information was first explicitly discussed in the U.S. in *State v. Armstead*, 432 So. 2d 837 (La. 1983).
[25] *University of Regina v. Pettick*, [1991] SJ No. 88 (CA) (QL), 77 DLR (4th) 615.
[26] Ibid.

that an expert should be required to lay the foundation for *computer-generated* data.[27] Justice Macleod erred on the side of caution saying the "computer may intimidate and give an aura of reliability which is not justified. At this stage of computer generated evidence, opinion evidence will not be admitted which rests essentially upon a computer program and a system of analysis for which no foundation has been laid."[28] This decision shows Justice Macleod's unwillingness to receive ESI evidence without the proponent establishing a strong presumption of reliability for the computer system that produced the data. In the years following his decision, his weariness of ESI and its originating source has not been adhered to by his fellow justices. In *Whitby Landmark Developments Inc. v. Mollenhauer Construction Ltd.* (2000), Justice Lamek of the Ontario Superior Court of Justice remarked:

> Computer technology has advanced very rapidly in recent years. Computers and their capacities to store, sort and reproduce information have become widely accepted in all walks of modern life. Not surprisingly, that development has been reflected by an increasing willingness on the part of the Courts to accept computer-stored information as reliable - subject, of course, to question but *prima facie* reliable."[29]

Our findings showed the extent of dissent over this issue of computer-generated records:

> Researcher*: Do you consider computer-generated records to be hearsay?*
>
> Interviewee*: That has come up. Of course, that depends on the purpose for which the record is being introduced. There are instances where it comes up for just the purposes of saying "there has been a record on such-and-such a date." That, I don't think would be hearsay.*
>
> Researcher*: Computer logs, for example, that log access to files or human activity on the computer, but are generated as a by-product of the people working on the computer. Would those be considered hearsay?*
>
> Interviewee*: I don't know that that would be hearsay. Metadata is not hearsay. If you are getting metadata just to show this the time the document was created, this is when it was accessed, this is when it was opened. That's not hearsay, that's for sure.*

---

[27] J. Mann, *Computer Technology and the Law in Canada* (Agincourt, ON: Carswell, 1987) and David Bender, *Computer Law* (New York: M. Bender, 1978).
[28] *University of Regina v. Pettick*.
[29] *Whitby Landmark Developments Inc. v. Mollenhauer Construction Ltd.*, [2000] O.J. No. 3838 (ONSJ) (QL) at paragraph 31, 4 C.L.R. (3d) 1.

> Researcher*: There is another type of computer-generated record which really is the result of a procedure which is embedded within the computer. For example, the ATM records of a transaction that a person makes with the bank – they're all computer-generated, without human intervention in the sense that the computers are programmed to do that, ah, do you consider them still hearsay?*
>
> Interviewee*: Yes, we'd consider them hearsay in the sense that they're automated, but they're triggered by the human being sticking the card into the machine, and putting in the PIN and giving commands… the digital artifacts will show us that a human being did or didn't act. And, I mean – yes, all digital evidence is hearsay.*

But another interviewee disagrees:

> Interviewee: …*notwithstanding [computer-generated records'] existence as hearsay, such statements will and must be admitted into evidence.*

There appears to be no consensus about a distinction between computer-stored evidence and computer-generated evidence. Another interviewee argued that the former is certainly hearsay, and subject to all the normal rules, but computer-generated evidence is more complex and risky, and "should perhaps be submitted to the scrutiny of 'authentication'" by showing that they were generated by a system or process capable of producing a reliable result.

But not everyone considers computer-generated material to be a common source of evidence:

> Researcher: *Do you make any distinction between digital entities that are generated within the computer environment without any human intervention and those that are human-generated, um, files?*
>
> Interviewee: *Yes. Yeah, I mean, there's the obvious forensic artifacts that they will identify to us as machine-generated, and tell us the context if they have any relevance, but they're really looking for digital artifacts that are as a result of human actions.*
>
> Researcher: *Do you treat the two as separate kinds of evidence?*
>
> Interviewee: *Well, I mean, the ones that are machine-generated are very rarely evidence.*

Ken Chasse poses a radical question – are the hearsay, best evidence, and authentication rules necessary for digital evidence? He concludes that they are not – that the best evidence rule is no longer relevant, and the business record provisions must be rewritten. Furthermore, system integrity bridges the gap between legal and records management rules, and so the call for "system integrity" should require

compliance of electronic record systems with recognized standards of records management.

What we have learned: *There is uneven knowledge and understanding about the nature of digital entities and whether all digital entities function as documentary evidence.*

What we have learned: *There is no consensus about the application of the hearsay rule and its exceptions to all forms of digital evidence.*

Legal effect and functional equivalence

Canada has taken the path of functional equivalence with respect to statutory reform for digital evidence. The model *UECA*, upon which provincial and territorial electronic commerce acts are based, stipulates that the electronic nature of information shall not deny it legal effect or enforceability (the model legislation does not adopt the use of "digital" – this term appears only once, in the definition of electronic as "stored in digital form or in other intangible form."[30]) The basic elements of the *UECA* are 1. Information shall not be denied legal effect or enforceability because it is in electronic form; 2. Transactions will have legal effect when conducted in electronic form if both parties consent, either explicitly or implicitly to conducting their business by electronic means; 3. when there is a legal requirement for information to be in writing, this is satisfied for electronic information when the information is accessible for future reference and can be retained, and when the recipient has control over what becomes of the information; 4. Electronic signatures will have the force of law when they indicate intent to sign the document, and are associated in some way with the document.

The *UECA* and its progeny do not include all instruments, however. It expressly says that its provisions, giving functional equivalence to electronic documents and electronic signatures, do not apply to wills and their codicils; trusts created by wills or by codicils to wills; powers of attorney, to the extent that they are in respect of the financial affairs or personal care of an individual; documents that create or transfer interests in land and that require registration to be effective against third parties. All are denied legal effect if in electronic form.

Provincial legislation permits probate as valid wills of documents that do not meet the formal requirements of a duly executed will in paper form, as long as they show the intention to make a will. Herein lies a contradiction: the result of the provisions is uncertainty over whether or not a testator could make a valid will by email, but a

[30] Uniform Law Conference of Canada, "Uniform Electronic Commerce Act," available at http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1.

Saskatchewan court ruled that if the requisite testamentary intention is present, a testator could make a will in an e-mail.[31]

What we have learned: *Functional equivalence between digital and paper transactions can only be attained by expressly providing for it in particular statutes, rather than by exclusive reliance on implicit cross-reference in a separate, self-contained statute such as the Uniform Electronic Commercial Transactions Act.*

Legal requirements for writing

Legal requirements for written and signed documents can cause inefficiencies and increase costs. "Although businesses are adapting to the electronic environment, legal rules continue to stipulate that certain transactions or documents be in writing. Many see such legal requirements as an impediment to transacting business electronically" (Davies, 2008). Health care professions support these requirements. Are the requirements for written documents and manual signatures really in the public interest or are they protective of health professions?

The conflict is illustrated by a recent opticians case: *College of Opticians of British Columbia v. Coastal Contacts Inc.*, 2009 BCCA 459. In this case, the College sought an injunction against Coastal for accepting and filling orders for contact lenses from members of the public over the Internet. According to its regulations, the College argued that Coastal was in breach because prescriptions had to be in paper and from a licensed optician. The BCCA was sympathetic to the supplier as offering efficiencies and less so to the College's concerns about accuracy and protecting the public. A majority granted the injunction but suspended it for 6 months to allow Coastal time for developing a compliant business. The dissenting appellate judge would have refused the injunction. The case identifies a bottleneck where paper required by a professional group creates inefficiencies in the delivery of health care. In the BCSC Coastal relied on the *Electronic Transactions Act*, s. 15(1) for the proposition that the seller is entitled to rely on the purchaser's acceptance of its terms. This was not disputed – the point was breach of the College's regulations.

Search and seizure

> Researcher: *Are there concerns, such as confidentiality or privilege, which may affect the scope of the digital material?*
>
> Interviewee: *That's a big issue. If somebody is getting access to the other party's hard drive for the purposes of gathering potential evidence, on that hard drive there is often the likelihood that there will be a mix of irrelevant, relevant , and*

[31] *Re Buckmeyer Estate*, 2008 SKQB 260, [2009] 1 WWR 142, related proceedings 2008 SKQB 141, [2008] 9 WWR 682.

privileged information. You've got to sort out an order where that is protected, which is not necessarily an easy thing.

As with all the issues raised in respect of digital evidence, in the interviews we conducted, there was no consensus about the degree of risk to personal privacy that may exist when a hard drive or other storage device is searched for potential evidence. Some of our interviewees saw this as a serious and unresolved issue. Others disagreed.

> Researcher: *Are there concerns, such as confidentiality or privilege, which may affect the scope of the digital material?*
>
> Interviewee: *Privilege very occasionally. In terms of confidentiality, it's an issue if it's a shared computer… we do our best to preserve confidentiality, but, bottom line is we've got a job to do so we basically just plow through it.*

In an investigation involving traditional sources of evidence, a warrant to search a premise is issued because of a reasonable expectation that material sought in evidence of the matter at issue will be found. There are strict guidelines to how that search is to be conducted, and how found material must be handled. In essence, the search takes place and then the potential evidence is seized. In the case of digital investigations, this process is turned upside down. While no warrant will be issued without a presumption that relevant evidence will be found, it is impossible to search without first seizing the computer or computers that are a source of suspicion or taking an image of the hard drive without accessing (and therefore searching) its contents.. This raises the fear of overly intrusive search and seizure of computers which conflicts with the need for limits to protect privileged communications, privacy and confidentiality. The issue affects:

(a) civil cases (e.g., *Celanese Canada Inc. v. Murray Demolition Corp*., 2006 SCC 36, [2006] 2 SCR 189 (imposing limits on civil search and seizure of computers in business premises pursuant to *Anton Piller* Orders to protect confidential communications between lawyer and client) (British Columbia Law Society, 2010);
(b) professional disciplinary cases (British Columbia Law Society, 2009); and
(c) criminal cases (e.g., *R. v. Morelli*, 2010 SCC 8, [2010] 1 SCR 253. This case involved a search warrant authorizing search of a personal computer for child pornography, but the defendant successfully challenged the evidentiary basis for the issuance of the warrant. The majority of the Court said: "The repute of the administration of justice would nonetheless be significantly eroded, particularly in the long term, if such unacceptable police conduct were permitted to form the basis for so intrusive an invasion of privacy as the search of our homes and the seizure and scrutiny of our personal computers"(at paragraph 103.)

What we have learned: *On the whole, Canadian law reform agencies are eager to bring laws up to the digital era but require further research and expertise to inform their recommendations.*

Are there really any problems?

Despite growing evidence of the disjuncture between the Canadian legal frame work and our increasing reliance on digital technologies, not all legal professionals perceive a problem with the laws as they are currently drafted. Several interviewees revealed this point of view.

> Researcher: *Do you think that the laws of evidence as they stand today are adequate to deal with digital material?*
>
> Interviewee: *The answer to this question is debatable.*

We must consider the potential risk inherent in the attitude that the current rules are entirely, or even somewhat adequate to deal with digital evidence. This attitude may be attributable to the fact that there is little case law in Canada that is moving legal thinking forward with respect to digital evidence. However, this is in sharp contrast to opinions of legal practitioners and scholars who engage in the challenges of digital technology daily, and find that we are "in the middle of a revolution as profound as the invention of the steam engine" (Davies, 2008). "Perhaps it is not being too unkind to say," concluded one interviewee, that "'willful blindness' underlies the view that says, 'we haven't had any problems.'"

3. Conclusion

The nature of electronic records challenges traditional rules of evidence and procedure. The traditional best evidence rule is no longer relevant because of the absence of originals in the digital environment. The authentication rule also is inadequate, because it cannot be established that an electronic record is the same as its first instantiation simply by looking at the record itself, but it is necessary to refer to an unbroken line of traces left by all those who interacted with the record or to the legitimate custody of a professional who can account for them (MacNeil, 2000; Duranti and Thibodeau, 2006; Duranti, 2009). Furthermore, the complexity and variety of digital information systems and the often uncontrolled ways in which they are used makes it difficult to identify records within them and the business activities to which they are linked, thereby challenging the application of the business records exception to the hearsay rule. Finally, ever-changing technology speeds up the obsolescence not only of earlier record-making processes, but also of the laws regulating admissibility.

Our research has shown clearly that inconsistencies in the law arising from a catch-up approach to the challenges introduced by information and communications technologies does not serve the standard of fair trial. This project has highlighted the problems inherent in laws developed over decades and centuries to account for traditional physical evidence to the vast array of electronic materials offered into evidence. Further research is required to develop proposed solutions that bring together the findings of international research into the nature of digital objects and advanced legal scholarship.

In 2007, the International Data Corporation predicted that "virtually all evidence brought before a court within the next three years will be from a digital source" and in 2008, the organization estimated that by 2013 the digital universe will be 10 times bigger.[32] If our laws cannot accommodate digital evidence in a manner that is fair and just – and consistent – then we will have rough justice indeed.

[32] The International Data Corporation (IDC): http://www.idc.com/home.jsp.

Appendix I

Definitions from Rules of Court

Jurisdiction and Title	Rule Number	Definition
British Columbia Supreme Court Civil Rules, BC Reg 168/2009	1-1(1)	"**document**" has an extended meaning and includes a photograph, film, recording of sound, any record of a permanent or semi-permanent character and any information recorded or stored by means of any device;
Alberta Rules of Court, A Reg 124/2010	5.14(3) Appendix	The Court or a party to an action who receives a computer-generated document that was filed with the court clerk may request the person filing that document or causing it to be issued to provide a copy of it in an electronic format. "**record**" includes the representation of or a record of any information, data or other thing that is capable of being represented or reproduced visually or by sound, or both;
Saskatchewan, *The Queen's Bench Rules*	211	… "**document**" includes information recorded or stored by means of any device and includes an audio recording, video recording, computer disc, film, photograph, chart, graph, map, plan, survey, book of account or machine readable information.
Manitoba, *Court of Queen's Bench Rules*, Man Reg 553/88	30.01(1)(a)	"**document**" includes a sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account and information recorded or stored by means of any device;
Yukon, *Rules of Court*	25(1)	"**Document**" includes a sound recording, videotape, photograph, chart, graph, map, plan, survey, book of account, and data and information in electronic form.
Northwest Territories, *Supreme Court Rules*	218(1)	…"**document**" includes a sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account and information recorded or stored by means of any device.
Ontario, *Rules of Civil*	1.03(1)	…"**document**" includes data and

Procedure, RRO 194/1990		information in electronic form; "**electronic**" includes created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means, and "**electronically**" has a corresponding meaning
Nova Scotia *Civil Procedure Rules*	14.02(1)	"**document**" means a document that is not electronic information, including a print version of electronic information and a non-digital sound recording, video recording , photograph, film, plan, chart, graph or record; "**electronic information**" means a digital record that is perceived with the assistance of a computer as a text, spreadsheet, image, sound, or other intelligible thing and it includes metadata, and all of the following are examples of electronic information: (i) an e-mail, including an attachment and the metadata in the header fields showing such information as the message's history and information about a blind copy, (ii) a word processing file, including the metadata such as the metadata showing creation date, modification date, access date, printing information, and the pre-edit data from earlier drafts, (iii) a sound file including the metadata, such as the date of recording, (iv) new information to be produced by a database capable of processing its data so as to produce the information; "**exactly copy**" means to make an electronic copy of electronic information in such a way that the copy is a mirror image of the

		original in a computer, storage medium, or other source; "**storage medium**" means a thing on which electric information is stored other than a computer, such as a digital versatile disc, a backup tape and a hard drive removed from a computer.
Prince Edward Island, *Rules of Civil Procedure*	30.01(1)(a)	…"**document**" includes a sound recording, videotape, film, photograph, chart, graph, map, plan , survey, book of account and data and information in electronic form;
Newfoundland and Labrador, *Rules of the Supreme Court, 1986*		**…** "**document**" includes a sound recording, photograph, film, plan, chart, graph, and a record of any kind;

Appendix II

Definitions from Interpretation Acts

Jurisdiction and Title	Section Number	Definition
Canada, *Interpretation Act*, RSC 1985, c I-21	s 35(1)	…"**writing**", or any term of like import, includes words printed, typewritten, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in visible form.
British Columbia, *Interpretation Act*, RSBC 1996, c 238	s 29	…"**record**" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise
Alberta, *Interpretation Act*, RSA 2000, c I-8	s 28(1)(jjj)	"**writing**", "**written**" or any similar term includes words represented or reproduced by any mode of representing or reproducing words in visible form.
Saskatchewan, *Interpretation Act*, SS 1995, c I-11.2	s 27(1)	"**writing**" or a similar term includes words represented or reproduced by any mode of representing or reproducing words in visible form;
Manitoba, *Interpretation Act*, SM 2000, c 26, CCSM c 80	Schedule of Definitions	"**writing**" and similar expressions means the representation of words in visible form by any means;
Quebec, *Interpretation Act*, RSQ c I-16	N/A	N/A
New Brunswick, *Interpretation Act*, RSNB 1973, c I-13		"**writing**", or "**written**", or any term of like import includes words printed, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in a visible form;
Nova Scotia, *Interpretation Act,* RSNS 1989, c 235		
Prince Edward Island, *Interpretation Act*, RSPEI 1988, c I-8	s 26(x.i)	…"**record**" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical, or otherwise

Newfoundland and Labrador, *Interpretation Act*, RSNL 1990, c I-19	s 27(1)(hh)	"**writing**", "**written**" or a term of like import includes words printed, painted, engraved, lithographed, photographed, or represented or reproduced by a mode of representing or reproducing words in a visible form;
Yukon, *Interpretation Act*, RSY 2002, c 125	s 21(1)	"**writing**", "**written**" or any term of like import includes words printed, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in a visible form;
Northwest Territories, *Interpretation Act*, RSNWT 1988, c I-8	s 28(1)	"**writing**", "**written**" or any term of similar import includes words printed, typewritten, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in visible form;
Nunavut, *Interpretation Act*, RSNWT 1988, c I-8, as duplicated for Nunavut by s 29 of the *Nunavut Act*, SC 1993, c 28	s 28(1)	"**writing**", "**written**" or any term of similar import includes words printed, typewritten, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in visible form;

Appendix III

Canada's Electronic Transactions Acts

Jurisdiction	Year	Title
Canada	2000	*Personal Information Protection and Electronic Documents Act,* SC 2000, c 5
Saskatchewan	2000	*The Electronic Information and Documents Act,* SS 2000, c E-7.22
Nova Scotia	2000	*Electronic Commerce Act*, SNS 2000, c 26
Ontario	2000	*Electronic Commerce Act*, SO 2000, c 17
Alberta	2001	*Electronic Transactions Act*, RSA 2001, c E-5.5
British Columbia	2001	*Electronic Transactions Act,* SBC 2001, c 10
Manitoba	2001	*The Electronic Commerce and Information Act*, SM 2000, c 32, CCSM c 55
New Brunswick	2001	*Electronic Transactions Act,* SNB 2001, c E-5.5
Newfoundland and Labrador	2001	*Electronic Commerce Act*, SNL 2001, c E-5.2
Prince Edward Island	2001	*Electronic Commerce Act*, RSPEI 1988, c E-4.1
Yukon	2003	*Electronic Commerce Act*, RSY 2002, c 66

Appendix IV

Letter of Request for Interview

Request for Participation in an Interview

PROJECT TITLE: The Canadian legal framework for evidence and the Digital Economy: a disjunction? (The Digital Economy Project)
PROJECT FUNDING: Social Sciences and Humanities Research Council of Canada (SSHRC) Knowledge Synthesis Grants on the Digital Economy

Principal Investigator: Anthony F. Sheppard, Professor of Law, UBC
Co-Investigator: Dr. Luciana Duranti, Professor of Library, Archival and Information Studies, UBC

This letter is to request your participation in a study conducted by the Digital Economy project. Participation would involve one semi-structured interview that will take approximately one hour. Two researchers will ask a set of prepared questions, provided to you ahead of the interview, and record the answers.

The Digital Economy project synthesizes knowledge from international research on the nature of digital records and legal scholarship on evidence. It's purpose is to research the applicability of the existing evidence laws to the complex digital environment. The discreet objective is to identify and address any areas of weakness in existing laws of evidence and the implication for the Digital Economy.

I hope you will be able to participate, and look forward to hearing from you. If you are agreeable, please let me know if there would be some convenient times for us to come to your office in the next couple of weeks.

Best regards,

Corinne Rogers, MAS
Doctoral student
University of British Columbia
School of Library, Archival and Information Studies

Appendix V

Interview Protocol and Participants

We contacted court clerks and records managers in federal and British Columbia law enforcement and courts systems; civil and criminal lawyers and judges at all levels of the BC Courts; digital evidence specialists in investigative or academic roles.

Court clerks and records managers	
Contacted	12
Interviewed	9

Civil and Criminal Lawyers	
Contacted	14
Interviewed	11

Judges	
Contacted	5
Interviewed	1

Digital Evidence Specialists	
Contacted	5
Interviewed	4

All interviews were conducted with at least two researchers. Interviews were digitally recorded with permission, and interviewees authorized their participation on the recording. Recordings were transcribed and the transcriptions analyzed with content analysis in NVivo Qualitative Analysis software.

Appendix VI

Interview Questions for Legal Professionals

1. Digital records and issues of law

- Do you think the law is sufficient for addressing discovery issues and/or evidentiary issues when it comes to electronic evidence?
- Do you think that the laws of evidence as they stand today are adequate to deal with digital material?
- What are the challenges to admissibility in relation to digital material?
- Do you feel that changes made to the Law of Evidence in the last 10-12 years (inclusion of the Uniform Electronic Evidence Act federally and similar changes in provinces and territories) to include digital material have been sufficient?
- What do you make of the fact that these changes do not deal with the hearsay rule and the business records exception to the hearsay rule?
- Do you think that there should be specific provisions/guidance in the law for the way digital material has to be regarded to be admissible (i.e. with respect to the business records exception)?
- What about weight? Are there problems with the fact that weight is not part of considerations of admissibility?
- Does the best evidence rule have any relevance for digital materials?
- What about the authentication rule?
- Do you look to any other international jurisdictions, their statutes and case law, for guidance in handling digital/electronic evidence? (If Canadian legal professionals believe the law is inadequate to address electronic evidence, where would they look first to establish better principles?)

2. Treatment of digital records – Authenticity

- What do you consider to be digital records?
- Do you make a distinction between what is a record and what is not a record?
    - If so, what distinctions do you make? do you treat them in the same way?
- Please outline the role that you have when preparing a case in one or more of the following activities:
    - creation, collection, maintenance, use and/or preservation of digital records
- When would you consider digital records that you create or receive to be trustworthy?
- When would you consider a digital record to be authentic?
    - Therefore, what for you are the characteristics of an authentic digital record?
    - What do you consider necessary in order to establish the authenticity of digital records in order for them to be admissible evidence?

    - Do you have any written regulations or policies with respect to the above?
- Are there specific types of digital records/digital environments that constitute a special challenge with respect to authenticity?
- Do you think that there are specific challenges to the maintenance of digital records as authentic evidence?
    - Can you describe instances in which digital records became inaccessible for evidence purposes?
    - Can you describe instances in which digital records lost their trustworthiness as evidence over time?
    - What is the longest time span that you are aware of in which digital records used as authentic evidence needed to be maintained?

3. Identification (recovery and forensic treatment)

- Does a search warrant specify what type of digital evidence is sought?
- If you are requesting material for examination, how detailed are you with respect to the digital material that needs to be acquired by a Digital Forensics expert?
    - For example, do you ask for e-mails, phone lists, pictures, audit trail (re: access to websites, changes), metadata, etc.?
    - Do you typically ask for an image of the hard drive or a selection of files from it?
    - What forms, if any, do you use?
    - What do you include in the narrative?
- Are there concerns, such as confidentiality or privilege, which may limit or alter the scope of the search for digital material that you seek to bring into an investigation?
    - How are these concerns raised?
    - When such a concern is expressed how is it handled?
- Do you make any distinction between digital entities that are generated in a computer environment with human intervention (i.e. office documents) and those that are generated in a computer environment without human intervention? (i.e. transaction logs)
    - If yes,
        - Why and in which way?
        - What do you do to distinguish them?
        - Do you treat them as a separate kind of evidence?
- How do you establish whether privileged documents are present?
    - If they are, are they removed?
        - If yes,
            - How?
            - How is privilege protected?

4. Collection

- What sort of evidence do you need to establish the authenticity of collected records after they have been transported from the crime scene to the DF lab or extracted from systems under examination?
- What do you need documented during extraction to establish the correctness of the procedure?
- What do you need documented during extraction to establish a chain of custody?
- What do you need documented during extraction to establish authenticity?

5. Examination

- During this stage, do you (or the forensic examiner) begin by confirming the authenticity of the records?
- What steps are taken to guarantee their authenticity?
- What is your analysis methodology?
    - What tools/strategies do you use?
- Do you generate metadata in the course of your analysis?
    - If yes,
        - What kind/categories of metadata?
        - How are these metadata captured and how are they preserved?
- Do you preserve the original relationship between the records when selected entities are removed from the system?
    - If yes, how?
- Does the issue of privilege arise at this stage?
    - If yes, how is it handled?

6. Presentation

- Do you consider digital records to be hearsay? [refer to previous questions]
- If so, under what exceptions to the hearsay rule do you seek to have digital evidence admitted?
- Do you make a distinction between what is a record and what is not a record?
    - If so, what distinctions do you make? do you treat them in the same way? (How can evidence be submitted as hearsay if it is not acknowledged as a record at the outset?)
- How do you present the evidence?
    - How is evidence presented to the court?
    - How is it presented to the other side?
    - Are both sides cooperating?
- What, if any, guidelines for the presentation of evidence do the parties follow (e.g., Sedona Canada, Ontario Bar Guidelines)?
- How do you determine which of the extracted evidence is submitted to the courts?
    - What factors do you consider in this determination?
- What, if anything, accompanies the evidence submitted to the courts (e.g., the metadata added during analysis, a report of the analysis, a report of the extraction process)?

- Do requirements for submission and types of information accompanying the submission change depending on the type of material or the collection process?
- Has it ever happened that evidence presented was challenged as a misrepresentation of the defendant's records?
- Has the authenticity of the submitted evidence ever been questioned?
    - What triggers a dispute over the authenticity of the submitted evidence?
    - Do you predict that it will be increasingly questioned or not?
- Are there any obstacles, in addition to the ones already identified, to the submission of evidence?
    - If yes, what?
- Do you retain a copy of what you present?
    - If yes,
        - Where?
        - How?
        - How is it handled?

7. Management and Preservation

- Are you concerned about maintaining authenticity of these records over the long term?
    - Are there any explicit rules about maintaining authenticity over the long term?
- What is your procedure for the maintenance of the evidence package or other documents before submission to court and for its preservation after the trial?
    - What about for the original?
    - What about for the copy?
- After trial and possible appeal, who should be responsible for the preservation of the evidence package?
    - Where and how should the evidence package be kept and for how long?
    - For example, what would happen with all the court documents for a case such as the Air India trial or the BC Rail case?
- If multiple copies of the evidence package exist, how does the court determine which is considered the authoritative version?
    - Who keeps it?
- Do you generate management and preservation metadata?
    - Do you keep audit trails of management and preservation measures?
    - How is access to the material regulated and controlled (access privileges, passwords, encryption, etc.)?
- How do you deal with technological obsolescence, possible loss of accessibility and interoperability?
- What do you do with extracted digital material that is not included in an evidence package?
- What material is destroyed?
    - What material is retained?
- For appeals, retrials and unsolved cases that are revived, how do you connect the old evidence with new evidence?

8. Concluding Questions

- Do you think that there is a specific knowledge necessary for anybody who has to assess the authenticity of digital records?
- What knowledge and expertise would be desirable for DRF professionals?
    - How would you assess the quality of digital forensics expertise?
    - What qualifications or certifications do you think would convey the existence of such expertise?

Appendix VII

Selected Codes Used in Analysis of Sources

Code	Sub-code
acquisition	
admissibility rules	authentication rule
	best evidence rule
	business records exception to hearsay rule
	electronic signatures
	formats
	hearsay rule
	legal value
	standards
	system integrity
anton piller order	
archival records as evidence	
archives policies about access	
authentication	
authenticity, reliability and trustworthiness	
authoritative copy	
authority of a regulatory body to copy and access records of one of its members	
business records	retention of business records
certification	
chain of custody, chain of command	
challenges with digital evidence	
changing technology	
common principles in e-commerce legislation	
computer stored v computer generated	
contesting admissibility	
context	
custodian - trusted custodian	
definitions	authentication
	authenticity
	automated transaction
	automatic message system
	book
	certificate
	certification service provider
	communication
	computer
	data
	data message
	database
	document
	electronic

	electronic agent
	electronic commerce
	electronic communications
	electronic data interchange
	electronic document or record
	electronic documents system
	electronic records system
	electronic signature
	electronically stored information
	fragmented information
	information system
	record
	relying party
	secure electronic signature
	separate documents
	signatory
	signature
	technology-based document
	true copy
digital forensics	
digital signature-electronic signature	
digital to analog comparison	
diplomatics	
discovery and disclosure	
e-discovery	
electronic commerce	benefits
	challenges
	formation of contracts
	place of business
	status
	time
emerging issues	
essential competences	
evidence acts	business records provisions
	electronic evidence provision
evidence seizure	
evolution- legislative reform and case law	
expert evidence	
forensic attitudes	
forensic copy critical to evidence preservation	
forensic process and product - handling	
formats and media	
interjurisdictional issues	
juridical context	
legal requirements for records management	
linking digital-analog or old-new evidence	
litigation hold	
loss of accessibility	
loss of trustworthiness	

metadata part of the record
mode of transmission
nature of digital data
need for education
non-repudiation
normal disclosure
obsolescence
original
place of business
policies and procedures
presentation of evidence
preservation and maintenance
privacy, privilege and confidentiality
problems arising from forensic imaging
problems with digital evidence
procedural fairness
protection of confidential and privileged information
purpose and function of paper documents
rationales for legislation
record systems-paper, hybrid, electronic
records management
records professionals
risk
search seizure and warrants
security and access
social dimension of legal records
spoliation
standards
subjective v objective
submission of evidence to court
sufficiency of law
technical obsolescence
technology-specificity or neutrality
time and deemed receipt
treatment of evidence
- ability to retain
- admissibility
- collection and storage
- copies
- declaration of authenticity
- determination of relevance
- determination of sufficiency
- establishing chain of custody
- establishment of authenticity
- functional equivalence
- identification of privileged information
- integrity - records concepts v systems consepts
- legal effect
- requirement of original

requirement of signature
requirement of writing
weight
trusted digital repository
trusted third party
types of case involving digital evidence
types of digital evidence
types of digital records
types of document and records management systems
types of documents
types of electronic devices
types of evidence
unallocated clusters
unintended consequences
usual and ordinary course of business
verification
workflow
writing

Bibliography

Arkfeld, Michael R. (2006). *Electronic Discovery and Evidence*. Phoenix, AZ: Law Partner Publishing, LLC.

Bantin, Philip. (2002). "Electronic Records Management–A Review of the Work of a Decade and a Reflection on Future Directions." *Encyclopedia of Library and Information Science 71*, (sup. 3): 47-81.

British Columbia Law Society. (2010). "Draft Model Order for Seizure and Safekeeping of Evidence." Available online: http://www.lawsociety.bc.ca/publications_forms/notices/10-07-06_antonpiller.html (accessed 20 November 2010).

--------. (2009). "Forensic Copying of Computer Records by the Law Society: A Report of the Mirror Imaging Working Group." Available online: http://www.lawsociety.bc.ca/publications_forms/report-committees/docs/mirror-imaging.pdf (accessed 20 November 2010).

Burke, Todd J. et al. (2008). *E-Discovery in Canada*. Markham, Ontario: LexisNexis.

Buskirk, Eric Van and Vincent T. Liu. (2006). "Digital Evidence: Challenging the Presumption of Reliability." *Journal of Digital Forensic Practice*, *1*: 19-26.

Carrier, Brian. (2003). "Defining Digital Forensic Examination and Analysis Tool Using Abstraction Layers." *International Journal of Digital Evidence*, *1*(4). Available online: http://www.utica.edu/academic/institutes/ecii/publications/articles/A04C3F91-AFBB-FC13-4A2E0F13203BA980.pdf (accessed 30 November 2010).

Casey, Eoghan. (2007). "What Does 'Forensically Sound' Really Mean?" *Digital Investigations*, *4*: 49-50.

Chasse, Kenneth L. (2010). "Electronic Discovery in the Criminal Court System." *Canadian Criminal Law Review*, *14*(2): 111-180.

Cox, Richard. (2006). *Ethics, Accountability and Recordkeeping in a Dangerous World.* London: Facet.

Davies, Alysia. (2008). "The Development of Laws on Electronic Documents and E-Commerce Transactions." *Library of Parliament—Parliamentary Information and Research Service*. Available online: http://www2.parl.gc.ca/Content/LOP/ResearchPublications/prb0012-e.htm; (accessed 25 November 2010).

Duranti, Luciana. (2009). "From Digital Diplomatics to Digital Records Forensics." *Archivaria*, *68*: 39-66.

Duranti, Luciana and Heather MacNeil. (1996). "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project." *Archivaria* 42: 46-67.

Duranti, Luciana and Kenneth Thibodeau. (2006). "The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES." *Archival Science*, 6: 26-33.

Duranti, Luciana, Corinne Rogers and Antony Sheppard. (2010). "Electronic Records and the Law of Evidence in Canada: The *Uniform Evidence Act* Twelve Years Later." *Archivaria*, *70*: 95-124.

Finlay, Bryan, Marie-Andrée Vermette, and Michael Statham (eds.). (2010). *Electronic Documents: Records Management, E-Discovery, and Trial*. Aurora, Ont.: Canada Law Book.

Gahtan, Alan M. (1999). *Electronic Evidence*. Scarborough, Ontario: Carswell, Thomas Professional Publishing.

Government of Canada. (2005). "CAN/CGSB-72.34-2005: Electronic Records as Documentary Evidence." Gatineau, Canada: Canadian General Standards Board.

Hedstrom, Margaret. (1997). "Building Record-Keeping Systems: Archivists are not Alone on the Wild Frontier." *Archivaria*, *44*: 44-71.

Hrycko, Oleh. (2009). *Electronic Discovery in Canada: Best Practices and Guidelines*. Toronto: CCH Canadian Limited.

Iacovino, Livia. (2005). *Recordkeeping, Ethics and Law: Regulatory Models, Participant Relationships and Rights and Responsibilities in the Online World*. Dordrecht: Springer.

Lynch, Daniel J. and Ian Brenson. (1989). "Computer Generated Evidence: The Impact of Computer Technology on the Traditional Rules of Evidence." *Loyal University Law Journal*, *20*(4): 919-936.

MacNeil, Heather. (2000). "Providing Grounds for Trust: Developing Conceptual Requirements for the Long-term Preservation of Electronic Records." *Archivaria 50*: 52-78

Mason, Stephen (ed.). (2010). *Electronic Evidence.* 2nd edition. LexisNexis Butterworths.

Moses, Lyria Bennett. (2007). "Recurring Dilemmas: The Law's Race to Keep Up With Technological Change." *University of New South Wales Faculty of Law Research Series*, *21*, available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/UNSWLRS/2007/21.html (accessed on July 8, 2010).

Murray, Daniel R., Timothy J. Chorvat, and Chad E. Bell. (2008). "Taking a Byte out of Discovery: How the Properties of Electronically Stored Information Have Shaped E-Discovery Rules." *Uniform Commercial Code Law Journal*, *41*(1): 35–49.

Paul, George L. (2004). "The 'Authenticity Crisis' in Real Evidence." *Practical Litigator*, *15*(6): 45-52.

--------. (2008). *Foundations of Digital Evidence*. Chicago: American Bar Association.

Peritz, Rudolph J. (1986). "Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence." *Northwestern University Law Review*, *80*(4): 956-1002.

Pollitt, Mark and Sujeet Shenoi (eds.). (2006). *Advances in Digital Forensics: IFIP International Conference on Digital Forensics*. New York: Springer.

Sedona Canada, Sedona Conference Working Group 7. (2008). "The Sedona Canada Principles: Addressing Electronic Discovery." *The Sedona Conference*.

Shilling, Cameron G. (2006). "Electronic Discovery: Litigation Crashes into the Digital Age." *The Labor Lawyer*, *22*(2): 207-232.