# INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION

**69th Annual Conference**
**October 3-6, 2004**




# Canadian Section Meeting

## KEEPING YOUR FINGER ON THE DIGITAL PULSE:

### CURRENT ISSUES IN DOCUMENT MANAGEMENT

*by*
Ralph G. Hildebrand

Deputy City Solicitor, City of Surrey




This is an informational and educational report distributed by the International Municipal Lawyers Association during its 69th Annual Conference, held in San Antonio, Texas, October 3– 6, 2004. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

## WHAT IS DOCUMENT MANAGEMENT AND WHY DO WE CARE?

### *THE HYPOTHETICAL*

Your municipality is involved in litigation regarding a sinking house. The building permit was issued 5 years ago and the house is now settling causing extensive damage to walls, windows, floor and roofing materials. At the time the building permit was issued there appeared to be no indication in the City's records that there were any problems with the subsurface conditions and no special engineering requirements were placed on the construction.

Litigation has started and the City has been served with a Demand for Discovery of Documents and you are trying to obtain copies of all documents related to the construction. The simple request for relevant documents has resulted in a perplexing array of responses from different departments at City Hall. Building sends you an address file but it contains no information regarding the history of the site before it had an address. Planning sends you bits of a correspondence file related to the rezoning of the property. Engineering and Clerks advise you that they have no information on file, even though roads were built as part of the rezoning and development of the lands and apparently City Counsel had something to do with the rezoning. No departments send you any digital documents, emails or voice messages.

### *OLD SCHOOL DOCUMENT MANAGEMENT*

At one time document management involved the creation of an alpha-numeric filing system that was utilized throughout the whole municipality. This system, while theoretically efficient, has implementation difficulties. The system is only as good as the people using it. A paper filing system works well as long as there is sufficient physical space to store the files, as long as people file the papers that came across their desks and as long as people used the system correctly. Misfiling is, unfortunately, not uncommon. Nor, tragically enough that three stage-desk-credenza-floor- filing technique which requires all correspondence, reports and related deleterious paper to remain in an office on either the desk, the credenza or the floor depending on its age or importance. Confusion over the numbering system results in whole files disappearing into a vacuum.

As the use of computers has grown, the amount of paper produced as grown exponentially: rather than becoming the paperless office we have the papered office. The result is that paper production outstrips storage and misfiling becomes increasingly common. The solution for storage issues was the advent of microfilming. However, with microfilming document searching became increasingly difficult.

"Old school" document management involving the handling of physical paper from creation until destruction with possibly some intermediary microfilming is quickly being outstripped by sheer volume and concomitant human error. In this context, technology is not just a fad, it is a fact that municipalities need to come to grips with in order to more efficiently create, circulate and store documents.

### *DOCUMENT MANAGEMENT > RECORDS MANAGEMENT*

Document management is more that merely archiving and storing records. It involves the flow of the document from its birth to its death. It is more than merely creating a digital file structure to mimic a physical file structure. Moreover, document management must deal with documents sent to the municipality as well as those created by the employees of the municipality.

A document management system must be inclusive and comprehensive despite changing technology. Emails, voice messages, Blackberry messages, photographs and maps are documents too and need to be incorporated into the document management system. The document management system needs to address legislated retention and disposition requirements, contain effective search and retrieval mechanisms and must encompass imaging and optical character recognition. In addition, in order for documents to be trustworthy, both for working purposes and for litigation purposes, there must be a high level of security and reliability built into the system.

The purpose of this paper is to take a brief look at some of the issues that need to be considered in implementing a "modern" digital document management system.

**THE LAW**

The issues that need to be considered first are, (1) When will digital documents be admitted in evidence as business records, (2) What are the criteria for production of business records and (3) what records must be produced.

To some extent the legal problem arises from a preliminary issue in digital documents as to what is the original and what is the copy for the purposes of the *Canada Evidence Act*. This issue was considered in *R. v. Vanlerberghe* (1978), 6 C.R. (3d) 222 (B.C.C.A.). In that case the court considered whether computer print outs from various branches of the Royal Bank were original documents or whether they were copies of the original, which were located in the computer. In considering section 30 of the *Canada Evidence Act* R.S.C. 1970 c. E-10 (admissibility of business records) the appeal court stated at page 224:

> *I think that the section clearly covers mechanical as well as manual bookkeeping records and the keeping of records, and the flowout or printout of that bookkeeping system clearly falls within the meaning of 'records' in s.30 and was therefore admissible.*

In *R. v. Bicknell* (1988) CarswellBC 781 (B.C.C.A.) the court again considered whether a print out was a copy and not properly proven pursuant to s. 30 and concluded that it was a record and not merely a copy.

While section 30 of the *Canada Evidence Act* remains relatively unchanged in the current iteration of the *Act*[1] other sections have been added to bring more clarity to the ramifications of modern technology.

Section 31.2 of the *Canada Evidence Act* R.S. 1985, c. C-5 deals with the best evidence rule and states:

> **31.2** (1) The best evidence rule in respect of an electronic document is satisfied
>
> (*a*) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
>
> (*b*) if an evidentiary presumption established under section 31.4 applies.

[1] See Schedule 1

(2) Despite subsection (1), in the absence of evidence to the contrary, an electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.

2000, c. 5, s. 56.

Provincial statutes have also addressed the issue of electronic documents.[2] The common theme for these statutes is to permit the storage of documents in electronic form and then to legislate to one extent or another the terms under which electronic documents may be admitted in court despite the best evidence rule. Many of the statutes refer to digital signatures, which, except for New Brunswick, means more than merely the digitization of a handwritten signature.

**SECURE ELECTRONIC SIGNATURES**

With the spread of electronic storage there is increased concern with respect to integrity of storage systems. Documents can be readily manipulated and altered at any workstation. How then can one ensure that the distinct goals of ease of access (search and retrieve functions) are met and at the same time ensuring the integrity and authenticity of the digital documents (would the original document please stand up)? There are a couple of preliminary points that need to be made about the documents created on desk top applications.

First, whenever a document is created attached to that document is "metadata". Metadata is data about the document. That document is stored in the document file itself and can be retrieved. So, for example, the metadata will contain information about the author of the document, the data it was created, the data it was altered and changes that have been made to a document. As a document is worked on more metadata is created and the file grows. For lawyers this creates a number of pratfalls. For example, if you create a List of Documents in Word and determine to remove a document from the list, when you subsequently email the List of Documents to the opposing counsel it may be possible for that counsel to deconstruct the file and ascertain what changes were made to the list. This might result in accidental disclosure of privileged information.

Probably the most infamous metadata story hit the press in 2000. A Democrat running for the U.S. Senate in Minnesota started receiving e-mails with Word documents attached criticizing and attacking the candidate. The e-mails and documents were anonymous until the metadata was inspected and it was discovered that they were authored by the chief-of-staff of the Republican incumbent.

The bad news about metadata is that there is no way to manually scrub all the data out of a file. However, there are applications that will do the job for you. Metadata Assistant and Workshare Metawall clean up documents made in Word, Excel and Powerpoint. In addition, if you attach a document to an email these programs can be programmed to automatically remove all of the metadata in the attached files.

Second, it is possible to alter those documents such as PDF files that are purportedly free of desktop manipulation. Forget about complicated document manipulation, all that is needed is a good scanner with a current OCR program. The steps are easy. Print the PDF file, scan and OCR it, correct any formatting or text errors, make the changes you want and save it as a PDF with the same name in the same directory.

[2] See Schedule I for some details regarding provincial legislation in this field.

One way of ensuring the authenticity of a document is to rely on a signature. In the world of paper documents a signature is an indication that a particular individual has approved a document or agreed to its contents. We take a written signature to indicate knowledge and intent. Moreover, the greater the ramifications of the signature the more formal the execution process.

A signature may be any mark but it must identify the person and contain within it an understanding that the person meant to sign the document. "Signature does not necessarily mean writing a person's Christian and surname, but any mark which identifies it as the act of the party." *Morton v. Copeland* (1855) 16 CB 517 at 535, per Maule J.

The problem with digital documents is that while each computer has a unique electronic signature, there is no way to establish the link between a particular person and the computer. Additional evidence is required. So, how do you prove that the electronic signature is the act of a real live person who intended to sign the record and that the record has not been altered? To describe the problem simply one need only think back to what was learned in law school regarding the doctrine of "*non est factum*".

The digital response has been to create digital signatures known as secure electronic signatures. The security arises from more than merely the attachment of a mark on a document. The signature is in reality a process of establishing the authenticity of a document which makes it reliable not only in terms of stored documents but also in the internet context.

By definition the internet is not intended for confidential or secure transactions or communications. There is however an increasing business need to expand the usefulness of the internet by providing confidentiality and security. Thus there is a need to augment the security of the internet. The security provided on the internet can also translate into security for documents by the use of secure electronic signatures.

The term "secure electronic signature" is defined in PIPEDA. PIPEDA provides a framework for electronic alternatives to paper based means of communicating The Act describes the characteristics of a "secure electronic signature" as:

1. Unique to the person;
2. Sole control of the person;
3. Used to identify the person; and,
4. Linked to the document and can determine if the document has been changed.

### *SECURE ELECTRONIC SIGNATURE PROCESS*

The manner in which the secure electronic signature process works is as follows:

1. The security program applies a hash function to data or a document to generate a message digest;
2. A private key is used to encrypt the digest;
3. The program attaches the encrypted digest to the electronic document of 1;
4. Using the internet the electronic document and encrypted digest and digital signature certificate (or means of access to it) are transmitted to a recipient;
5. After receipt of the items in (4):

a. The public key contained in the certificate is used to decrypt the encrypted digest and produce the digest in (1);
b. The hash function is applied to the data in the electronic document to generate a new digest;
c. The program verifies that the digests in (1) and (b) are identical; and,
d. Verification is completed to ensure that the digital signature certificate is valid.

### *DIGITAL SIGNATURE CERTIFICATES*

A digital signature certificate is valid if, at the time when the data contained in an electronic document is digitally signed, the certificate is:

(a) Readable by any person entitled to have access to it and
(b) Has not expired or been revoked.

Digital signature certificates, together with the public and private keys are issued by private companies who have received certification authority from the President of the Treasury Board who verifies that:

- The CA has the capacity to issue certificates in a secure and reliable manner within the context of the Regulations; and,

- The characteristics of Secure Electronic Signatures produced by the CA match those specified in the Act.

You can locate some helpful links regarding secure digital signatures at http://www.solutions.gc.ca/pki-icp/guidedocs/guidedocs_e.asp

### *HOW TO GET AND USE A SES*

1. Get a private and a public key pair

2. Go to a Certification Authority recognized by the GoC.

3. Get a Digital Certificate:

    - The CA will sign and publish the Digital certificate

    - The certificate guarantees that the public key is really associated with your private key

    - Step 1,2&3 may be combined – the CA may issue the keys and the digital certificate

4. Then, when required, use your private key to create your secure electronic signature.

5. When someone checks your signature they will also check

    a. The digital certificate

b. And the government web site to see if the CA is listed.

6. If both are OK they can trust that you signed the document and that it hasn't been changed since you signed it.

How does this process increase in house document security and reliability? As more documents and contracts will be received over time using SESs, there will be a need to ensure that document storage includes storage of the related digital certificates. Both must be accessible to prove that authenticity and reliability of documents.

Having found that there can be secure and reliable documents, how can you make sure that you can access them when you need to?

## RECORD/DOCUMENT MANAGEMENT STANDARDS

A wide variety of document management systems are available. Laserfiche, Hummingbird and PCDocs are all products providing document management. What are you looking for in a document management product?

| | |
|---|---|
| **Authenticity** | Providing records that are verifiably accurate, trustworthy and reliable |
| **Completeness** | Capturing and preserving the original content, context and structure of the information |
| **Integrity** | Records are protected against alteration or deletion while retained |
| **Retention** | Achieving full compliance with retention requirements including "hold orders" |
| **Official Copy** | Having on "official copy" of records with copies governed by different business rules |
| **Accessibility** | Delivery of all related information quickly, regardless of format |
| **Recovery** | Records are automatically duplicated, retained at a remote site |
| **Audit** | The "chain of custody" can be tracked and management evidence produced to prove the negative |

Part of the process of determining the product which fulfills the requirements of your organization should include a review of the American Product Register. A Product Register is maintained by the U.S. Department of Defense. That Register sets out DoD requirements and standards for document management systems. The standard was recently updated and is set out in DoD 5015.2STD, June 2002 - Department of Defense (DOD) 5015.2 – STD certification for Electronic Records Management Software Applications. Applications that have been granted 5015.2 certification must meet rigorous requirements for systematic control of the creation, maintenance, use, reproduction, and disposition of records for the purpose of regulatory and legal compliance. Needless to say, it is highly likely that the DoD standard includes all of the

necessary elements that will be considered at the local government level regarding documents security and integrity.

This Standard sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by DOD Components in the implementation of their records management programs; defines required system interfaces and search criteria to be supported by the RMAs; and describes the minimum records management requirements that must be met, based on current National Archives and Records Administration (NARA) regulations. The Product Register includes information on the product, the test configuration and a summary report.

At the end of the day, the decision regarding which of the document management systems will best serve the needs of your organization is a function of those needs, the climate of the organization and budgetary considerations. Certainly it is recommended that where possible local governments should work together to attempt to create economies of scale to make document management systems more affordable and should share information gained through implementation and use of specific products.

**US NEW DIGITAL DISCOVERABILITY RULES**

With increased digital storage there is a need for increased discovery. To date there has not been wholesale rewriting of the rules of discovery to set the parameters of digital discovery. However, there has been a fair bit written on the requirements under the existing rules to produce all documents including digital documents and, in some cases, to produce the actual hard drives.

In the United States the Bar is coming to grips with a rewriting of the rules to deal with digital document discovery. The U.S. Federal courts have proposed draft rules for "E-Discovery" which attempt to recognize the difficulties and challenges of producing digital data.

The draft rules, published on Aug. 15 by the Advisory Committee on Federal Rules, address such issues as inadvertent disclosure of privileged information, treatment of information that is not reasonably accessible and consequences of loss or destruction of electronic data.

The most controversial of the proposed rules may be an amendment to Rule 37 that would create a narrow "safe harbor," protecting a party from sanctions for failing to provide electronically stored information in some circumstances. Under the proposed amendment a party would be protected if it "took reasonable steps to preserve the information after it knew or should have known the information was discoverable ... and the failure resulted because of the routine operation of the party's electronic system." The party must also not have violated any court order requiring it to preserve electronically stored information.

The proposed amendment is meant to deal with the fact that electronic data can disappear in cyberspace without anyone trying to destroy it, through programs that automatically recycle data, overwrite deleted information and discard data that has not been accessed for a certain period. This arises because every time a computer is turned on some data is being overridden.

There are also proposed are changes to Rules 26 and 45 (privilege rules), which are prompted by concern that electronically stored information can be so voluminous and so much more difficult to review that it increases the risk privileged material will slip through and be inadvertently turned over in discovery.

A new subsection (B) to Rule 26(b)(5) provides that a party who produces privileged material without intending to waive the privilege, may, "within a reasonable time," notify the recipient, who would have to "promptly return, sequester, or destroy the specified information and any copies." The producing party would have to prepare a privilege log and otherwise comply with existing rules on withholding privileged material.

The proposed Rule 45 revision sets up similar requirements for subpoenas. However, the draft rules merely set out a procedure for dealing with privilege waiver issues, leaving it with the courts to decide whether waiver has occurred.

Parties sometimes enter into agreements that allow for essentially the same procedure, enabling them to turn over documents without review and retrieve anything that turns out to be privileged. They are known as "quick peek" and "clawback" agreements.

A third major area addressed by the proposed rules involves how to deal with discovery of data that is not readily accessible -- for example, "legacy data" currently unused and stored on an obsolete system, deleted data and inactive data stored for disaster recovery purposes. A typical example would be information wiped from a computer hard drive on an employee's departure. The data can be recovered but it takes time and money.

An amendment to Rule 26(b)(2) would provide that such information need not be reviewed or turned over. But if an adversary moves for disclosure, the party would have to show the information was "not reasonably accessible." The court could then require disclosure only for good cause and on specified terms and conditions.

In addition, proposed changes to Rules 33 and 34 would:

- Distinguish between electronically stored information and documents, meaning that parties requesting discovery would have to specify whether they are seeking documents, electronic data or both.

- Clarify that an answer to an interrogatory involving business records should involve a search of electronically stored information.

- Allow a responding party to substitute access to electronically stored data for an answer only if the burden of deriving an answer is substantially the same for both sides.

- Allow parties seeking discovery to specify the form of production for electronic information and allow those disclosing to object to the form.

- Provide that where there is no request, agreement or court order specifying the form of production, a producing party would be allowed to produce information either in the form it is ordinarily maintained or in an electronically searchable form.

- Clarify that the obligation to produce for testing and sampling also applies to nonelectronic discovery.

**CONCLUSION**

The power of the computer has been the opportunity and ability it creates to allow anyone to publish perfect documents, newsletters, spreadsheets, memoranda etc. With the increased ability there has been increased production of such documents with related storage, security and retrieval issues. Document management systems are needed to track and secure documents from creation to final destruction. Digital security is needed to establish for both court purposes and practical purposes, which digital document is the original signed and sealed manifestation of agreement, intend or direction. While powerful software programs have been created to assist in these endeavours, one needs to keep abreast of both the software solutions and the problems they create in order to protect and preserve local governments' corporate knowledge, which knowledge stored in many documents may be either a boon to corporate governance or a minefield.

## SCHEDULE 1

**Canada Evidence Act- PART I**

Business records to be admitted in evidence

**30.** (1) 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.

Inference where information not in business record

(2) Where a record made in the usual and ordinary course of business does not contain information in respect of a matter the occurrence or existence of which might reasonably be expected to be recorded in that record, the court may on production of the record admit the record for the purpose of establishing that fact and may draw the inference that the matter did not occur or exist.

Copy of records

(3) Where it is not possible or reasonably practicable to produce any record described in subsection (1) or (2), a copy of the record accompanied by two documents, one that is made by a person who states why it is not possible or reasonably practicable to produce the record and one that sets out the source from which the copy was made, that attests to the copy's authenticity and that is made by the person who made the copy, is admissible in evidence under this section in the same manner as if it were the original of the record if each document is

(*a*) an affidavit of each of those persons sworn before a commissioner or other person authorized to take affidavits; or

(*b*) a certificate or other statement pertaining to the record in which the person attests that the certificate or statement is made in conformity with the laws of a foreign state, whether or not the certificate or statement is in the form of an affidavit attested to before an official of the foreign state.

Where record kept in form requiring explanation

(4) Where production of any record or of a copy of any record described in subsection (1) or (2) would not convey to the court the information contained in the record by reason of its having been kept in a form that requires explanation, a transcript of the explanation of the record or copy prepared by a person qualified to make the explanation is admissible in evidence under this section in the same manner as if it were the original of the record if it is accompanied by a document that sets out the person's qualifications to make the explanation, attests to the accuracy of the explanation, and is

(*a*) an affidavit of that person sworn before a commissioner or other person authorized to take affidavits; or

(*b*) a certificate or other statement pertaining to the record in which the person attests that the certificate or statement is made in conformity with the laws of a foreign state, whether or not the certificate or statement is in the form of an affidavit attested to before an official of the foreign state.

Court may order other part of record to be produced

(5) Where part only of a record is produced under this section by any party, the court may examine any other part of the record and direct that, together with the part of the record previously so produced, the whole or any part of the other part thereof be produced by that party as the record produced by him.

Court may examine record and hear evidence

(6) For the purpose of determining whether any provision of this section applies, or for the purpose of determining the probative value, if any, to be given to information contained in any record admitted in evidence under this section, the court may, on production of any record, examine the record, admit any evidence in respect thereof given orally or by affidavit including evidence as to the circumstances in which the information contained in the record was written, recorded, stored or reproduced, and draw any reasonable inference from the form or content of the record.

Notice of intention to produce record or affidavit

(7) Unless the court orders otherwise, no record or affidavit shall be admitted in evidence under this section unless the party producing the record or affidavit has, at least seven days before its production, given notice of his intention to produce it to each other

party to the legal proceeding and has, within five days after receiving any notice in that behalf given by any such party, produced it for inspection by that party.

Not necessary to prove signature and official character

(8) Where evidence is offered by affidavit under this section, it is not necessary to prove the signature or official character of the person making the affidavit if the official character of that person is set out in the body of the affidavit.

Examination on record with leave of court

(9) Subject to section 4, any person who has or may reasonably be expected to have knowledge of the making or contents of any record produced or received in evidence under this section may, with leave of the court, be examined or cross-examined thereon by any party to the legal proceeding.

(10) Nothing in this section renders admissible in evidence in any legal proceeding

(*a*) such part of any record as is proved to be

(i) a record made in the course of an investigation or inquiry,

(ii) a record made in the course of obtaining or giving legal advice or in contemplation of a legal proceeding,

Evidence inadmissible under this section

(iii) a record in respect of the production of which any privilege exists and is claimed, or

(iv) a record of or alluding to a statement made by a person who is not, or if he were living and of sound mind would not be, competent and compellable to disclose in the legal proceeding a matter disclosed in the record;

(*b*) any record the production of which would be contrary to public policy; or

(*c*) any transcript or recording of evidence taken in the course of another legal proceeding.

(11) The provisions of this section shall be deemed to be in addition to and not in derogation of

Construction of this section

(*a*) any other provision of this or any other Act of Parliament respecting the admissibility in evidence of any record or the proof of any matter; or

(*b*) any existing rule of law under which any record is admissible in evidence or any matter may be proved.

Definitions

(12) In this section,

"business" «*affaires*»

"business" means any business, profession, trade, calling, manufacture or undertaking of any kind carried on in Canada or elsewhere whether for profit or otherwise, including any activity or operation carried on or performed in Canada or elsewhere by any government, by any department, branch, board, commission or agency of any government, by any court or other tribunal or by any other body or authority performing a function of government;

"copy" and "photographic film" «*copie*» *et* «*pellicule photographique*»

"copy", in relation to any record, includes a print, whether enlarged or not, from a photographic film of the record, and "photographic film" includes a photographic plate, microphotographic film or photostatic negative;

"court" «*tribunal*»

"court" means the court, judge, arbitrator or person before whom a legal proceeding is held or taken;

"legal proceeding" «*procédure judiciaire*»

"legal proceeding" means any civil or criminal proceeding or inquiry in which evidence is or may be given, and includes an arbitration;

"record" «*pièce*»

"record" includes 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, and, except for the purposes of subsections (3) and (4), any copy or transcript admitted in evidence

under this section pursuant to subsection (3) or (4).

R.S., 1985, c. C-5, s. 30; 1994, c. 44, s. 91.

## SCHEDULE 2

B.C. ***Electronic Transactions Act*** (S.B.C. 2001) c. 10: Determines the conditions electronic transactions, permits records to be stored in electronic manner, permits business transactions to be completed using electronic signatures unless specifically prohibited by the Act, ie wills, land transactions etc.

***Evidence Act*** R.S.B.C. 1996, c. 124: Interestingly enough deals specifically with photographs including microphotographs and photocopies kept for a permanent record but only by extrapolation can you assume deals with digital photographs. Photographs need to be taken as "an established course of practice". However, with respect to business records a document includes any device by means of which information is recorded or stored and therefore if in the ordinary course of business records are stored digitally then they are admissible.

AB ***Electronic Transactions Act***, S.A. 2001, c. E-5.5 Similar to the B.C. *Electronic Documents Act,* in granting legal effect to electronic documents, permits the retention of records in electronic form and makes a specific reference to governments storing documents and records electronically (20), permits and regulates electronic payments (24). The *Act* was proclaimed in force on April Fool's Day 2003.

***Evidence Act***, R.S.A. 2000, c-18: Amendments to the *Act* in added sections 41.1-41.8 which permits electronic documents to be entered into evidence subject to findings of integrity with respect to the storage etc of the document. Viz. 41.6

> *For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, having regard to the type of business or endeavour that used, recorded or stored the electronic record and the nature and purpose of the electronic record.*

SA ***Electronic Information and Documents Act,*** 2000, S.S. 2000, c. E-7.22: Permits the storage of documents in digital form (15),

***Evidence Act***, R.S.S. 1978, c. S-16: The *Act* has been amended to permit the use of electronic documents (29.1-29.6) however they must be proved to be authentic, ie, it is what it claims to be (29.2), however the best evidence rule is met by establishing the integrity of the document

Ont. ***Electronic Commerce Act,*** 2000, S.) 2000, c. 17: Section 8 permits the storage of documents in electronic form subject to integrity and reliability requirements (8(2))

***Evidence Act***, R.S.O. 1990, c. E.23: There is an interesting provision which indicates, (contrary to the normal disclaimer regarding the "official document") that Government of Ontario statutes, regulations and related material that are available on the Internet at

www.e-laws.gov.on.ca are an accurate statement of the law(24.2). The provisions regarding electronic documents are found at s. 34.1

***Electronic Registration Act (Ministry of Consumer and Business Services Statutes)***, 1991, S.O. 1991, c. 44 amended by 2001, c. 9, Sched. D, s. 13: This ***Act*** is intended to permit persons who are required or permitted to file information under designated Acts to file such information in electronic formats.

QU ***Municipal Code of Quebec***, R.S.Q. c-27.1: Has provisions requiring municipalities to establish an electronic tendering system (938)

NB ***Electronic Transactions Act,*** S.N.B. 2001, c. E-5.5: This is the most "plain English" of the Acts. It stated purpose is to "facilitate the use and acceptance of electronic information by persons who wish to do so". Electronic documents are given legal effect (s. 6). Oddly enough the *Act* does permit an electronic signature to consist of an electronic representation of the manual signature of the person signing the document (s. 10(2)). Also a requirement to deliver by mail may be satisfied by email if the person sending requires a receipt of delivery and the person reply provides a receipt of delivery together with an electronic signature (s. 14)

***Evidence Act,*** R.S.N.B. 1973, c. E-11*:* Permits electronic documents to be used in court proceedings (s. 47.1-47.2)

NS ***Electronic Commerce Act***, S.N.S. 2000, c. 26

***Evidence Act***, R.S.N.S. 1989, c. 154: Electronic records are dealt with in section 23A-23H. However, the reference to business records includes "'record' includes any information that is recorded or stored by means of any device", and therefore arguably no amendments were needed to permit electronic records to be used for court purposes as long as they were produced in the ordinary course of business.

NL ***Electronic Commerce Act,*** S.N.L. 2001, c. E-5.2

***Evidence Act,*** R.S.N.L. 1990, c. E-16: Has no provisions regarding digital documents save and except for electronically filed government documents, (s. 29)