

**Managing
Intellectual
Property™**

*IP***Handbook**



**World IP Contacts
Handbook** 14th edition

2007

Using electronic records in patent proceedings

Electronic records are increasingly important as evidence in patent disputes. **Damien McCotter** and **Peter R Wilcox** of **Torys LLP** examine how Canada's federal and state authorities have regulated their use

In Canada, a patent granting exclusive property to a claimed invention can be obtained only if the applicant complies with all the requirements of the Patent Act (RSC, 1985, c P-4) and associated Patent Rules (SOR/96-423). As in most jurisdictions, Canadian patent law is founded on the fundamental requirements of novelty, utility and non-obviousness embodied in a proper public disclosure of the claimed invention.

Priority regarding patent rights in Canada is determined on the basis of which applicant first files an application. The Act provides that between two (or more) competing applications for the same invention, the one with the earliest claim date is entitled to the patent. Where disputes arise as to priority or patent validity, the facts relating to the invention process may become relevant during the course of proceedings before the Canadian Patent Office or the Canadian courts.

Documents generated by inventors and other scientists assisting the inventors are often introduced into evidence to provide the invention story, including who was involved in the invention and what was actually invented. The reliability and accuracy of any documentary evidence in support of the inventive process may be critical to proceedings in the Canadian Patent Office and the Canadian courts. Whether it is in the context of prosecution or litigation, the question is: "How do innovators in Canada properly evidence their inventive process?" This question becomes critical as society moves toward electronic storage of data. Canadian law has evolved to permit electronic documents in legal proceedings.

Evidence of invention

In laboratory settings, the inventive process has traditionally been documented through a formalized procedure of laboratory notebooks, hardcopy records management and invention disclosure statements. Lab notebooks typically record the date and names of the parties involved and chronicle any experimental procedures, results, observations and conclusions. In many cases, it is these experimental procedures and results that populate the specification of a patent application or are entered into evidence in a court proceeding.

Discovery of electronic documents

In the context of document discovery, electronic documents (lab notebooks or otherwise) fall under the definition of "document" in both the Federal Courts Rules (SOR/98-106) and the Ontario Rules of Civil Procedure (RRO 1990, Regulation 194). Under the Federal Courts Rules, "document" is defined as:

222 (1)... "document" includes an audio recording, video recording, film, photograph, chart, graph, map, plan, survey, book of account, *computer diskette and any other device on which information is recorded or stored* [emphasis added].

Under the Ontario Rules, the definition is similar:

30.01 (1)(a)... "document" includes a sound recording, film, videotape, photograph, chart, graph, map, plan, survey, book of account, and *data and information in electronic form* [emphasis added].

The general definitions in the Ontario

Rules further define “document” as including “data and information in electronic form” and “electronic” as including any document that is “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”.

What these definitions reveal is that not only does a traditional hardcopy record qualify as a document under the rules but so too does a softcopy electronic record. Any data or information stored in electronic form meets the definition of “document” and is thus subject to the documentary discovery provisions found in either the Federal Court Rules or the Ontario Rules.

However, satisfying the definition of document for the purposes of discovery does not alone guarantee that lab notebooks or other records (either in paper form or electronic form) will be admitted into evidence during a court proceeding. Under the laws of evidence in Canada, the court will consider the relevance and necessity of the proposed documentary evidence. The admissibility of relevant evidence is not a question of judicial discretion in Canada: if certain evidence is relevant, it is admissible. However, the court does have discretion regarding the weight that should be given to certain admissible evidence. In the context of documentary evidence, the court will consider the *authenticity, integrity and reliability* of the document when making a determination of the weight that it should be given.

Questions of authenticity, integrity and reliability are particularly pronounced when parties seek to tender electronic documents as evidence. Electronic documents by their nature are accessible, reproducible and easily manipulated. Businesses today accumulate vast amounts of electronic data and store multiple versions of numerous documents.

Networks provide access to an extensive number of users and provide varying degrees of security, or none at all. Concern about the authenticity, integrity and reliability of electronic documents, compared with a signed and dated lab notebook in the handwriting of a named inventor, can be appreciated.

Electronic evidence: proposed uniform statutes

Concern over these issues influenced the drafting of what is known as the Canadian Uniform Electronic Evidence Act [UEEA] in 1998 (which is not law) and the subsequent enactment of the Personal Information Protection and Electronic Documents Act (RSC 2000, c 5, [PIPEDA]). UEEA was drafted in 1998 by the Uniform Law Conference of Canada (ULCC), which assembles government lawyers, private lawyers, policy analysts and law reformers to consider areas in which provincial and territorial laws would benefit from harmonization. The ULCC adopts “uniform statutes” such as UEEA, and, where appropriate, recommends their enactment by the federal, provincial and territorial governments of Canada.

UEEA deals with the admissibility of electronic documents as evidence where the authenticity of the documents and the integrity of the electronic storage system can be demonstrated. Certain provisions in UEEA permit the introduction of evidence of any standard, procedure, usage or practice regarding the way the documents are recorded and stored. Evidence showing the integrity of the storage system may help determine whether the electronic documents tendered for admission should be received as authentic and reliable.

Uniform statutes formulated by the ULCC are not enforceable as Canadian law, but rather suggest to the federal, provincial and territorial governments the benefits of uniform legislation in certain realms. Both the federal

government of Canada and the provincial government of Ontario have since enacted provisions similar to those recommended in the UEEA.

For example, the federal government enacted PIPEDA in 2000 to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes individuals' right of privacy regarding their personal information. Part III of PIPEDA included the UEEA electronic evidence provisions as proposed amendments to the Canada Evidence Act (RSC 1985, c C-5[CEA]). In 2003, these amendments were incorporated into CEA.

Law of evidence regarding electronic documents

CEA applies to proceedings in the Federal Court of Canada and incorporates by reference the laws of evidence of the province in which the proceedings are initiated, except for laws inconsistent with or contrary to federal laws. The amendments regarding the admissibility of electronic evidence are in sections 31.1 to 31.8 of the CEA (with similar provisions found in section 34.1 of the Ontario Evidence Act (RSO 1990, c E.23, s 34.1)). CEA now defines (at 31.8) "electronic document" and "electronic documents system":

"[E]lectronic document" means 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. "[E]lectronic documents system" includes a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic documents.

The fundamental premise of the new

provisions is that the authenticity and reliability of electronic documents can be established by showing the integrity of the electronic documents system. The burden to do so rests on the party seeking to admit the electronic document:

31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

To legitimize the acceptance of electronic documents as evidence before the court, CEA had to reconcile such admission with the existing rules of evidence, including (1) hearsay, (2) best evidence, and (3) authentication. If a party wishes to admit printouts or other such "copies" of the original electronic record, it was thought that the rule of best evidence might be offended. The new CEA provisions have therefore resolved this concern by legislating a specific application of the rule to electronic documents:

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 [i.e., secure electronic signatures]. (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.

Under CEA, the best evidence rule does indeed apply to computer data but does so without impeding its admissibility. Where the

integrity of the electronic documents system is proven, the best evidence rule regarding an electronic document is satisfied, in whatever form the electronic evidence takes (for example, printout, magnetic hard drive, tape, semiconductor memory, optical storage). As proof of the integrity of the electronic documents system, CEA provides that certain standards can be considered by the court:

31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.

CEA provides for the admissibility of electronic evidence (where relevant); the strength with which its authenticity, integrity and reliability are demonstrated will affect the weight that the court gives the electronic evidence. The integrity of the procedures and standards incorporated in an in-house electronic documents system will bolster the weight of electronic evidence.

Electronic records as documentary evidence

On December 1 2005, the Canadian General Standards Board (CGSB) released a standard that outlines how to ensure that records generated from electronic information systems are reliable, authentic and trustworthy. The CGSB Standard on Electronic Records as Documentary Evidence (CAN/CGSB 72.34-2005 (December 1 2005)) was created over a three-year period to help public and private organizations facilitate the admissibility of electronic documents in legal proceedings. The standard is applicable to both electronic records created by an individual (such as

electronic lab notebooks) and those entered as a result of data interchange without intervention by an individual (such as automated test results).

The goal of the standard is for those in compliance to demonstrate formally certain key elements in order to prove an organization's "usual and ordinary course of business" and the integrity of the electronic documents system. These key elements include:

- contemporaneous recording of information and data;
- routine business data and routine data entry;
- reliance on the information and data by the organization;
- software reliability;
- processing verification of data and information in records;
- security and protection against unauthorized access to data and information;
- maintaining backup copies; and
- proper retention and disposition of electronic record.

If an organization can demonstrate to the court that its electronic documents system implements these standards, it is anticipated that any electronic documents recorded or stored in such a system will be deemed admissible on account of the proven integrity of the storage system. If relevant, the court will extend the appropriate weight to the evidence on the basis of demonstrated authenticity, integrity and reliability.

Electronic documents in the ordinary course of business

It is apparent that this standard was drafted to dovetail with not only the CEA provisions regarding electronic evidence (sections 31.1 to 31.8) but also the provisions dealing with the admissibility of business records. Section 30(1) of CEA deals with the recording of

information and data in the “ordinary course of business”:

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.

[...]

(3) Where it is not possible or reasonably practicable to produce any record described in subsection (1)... a copy of the record accompanied by two documents [i.e., affidavits], 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.

The legislation and the CGSB standard are formulated in this manner to address the hearsay rule. Documents that are prepared in the ordinary course of business alleviate the hearsay concern of reliability and thus may be admissible as business records to prove the truth of their contents. Softcopy computer records produced by user input in the ordinary course of business are covered by section 30(1) of CEA. Alternatively, if the original softcopy recording of the input was for some reason not available, a hardcopy computer printout would be admissible under section 30(3) if the affidavit requirements were met. Additionally, an automatic data collection system in a computer-based record-keeping system may be classified as original evidence or real evidence, which does not offend the hearsay rule either.

In a laboratory setting, the practical

implications of these “ordinary course of business” provisions are clear. If a lab employs a digital notebook procedure in the researcher’s ordinary course of business, the electronic contents of the notebook (in softcopy or printed hardcopy) would be admissible. Likewise, if automated test results are being generated and recorded in the ordinary course of business, these data would also be admissible.

If the lab work, though relevant, was not necessarily done in the ordinary course of business, any experimental notes or results could be alternatively admissible under the electronic evidence provisions of CEA so long as the authenticity of the electronic documents can be demonstrated and the integrity of the electronic documents system proven.

Secure electronic signatures

The authenticity of electronic documents can be further bolstered by the use of secure electronic signatures, as defined in PIPEDA (subsection 31(1)):

“[S]ecure electronic signature” means an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1).

48. (1) Subject to subsection (2), the Governor in Council may, on the recommendation of the Treasury Board, make regulations prescribing technologies or processes for the purpose of the definition “secure electronic signature” in subsection 31(1).

Section 48(1) of PIPEDA contemplates the issuance of regulations that require the use of specific technologies or processes for secure electronic signatures. Section 31.4 of CEA contemplates evidentiary presumptions regarding the association of secure electronic signatures with individuals, and the integrity of electronic documents signed with secure electronic signatures:

31.4 The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting (a) the association of secure electronic signatures with persons; and (b) the integrity of information contained in electronic documents signed with secure electronic signatures.

Under PIPEDA and CEA, the federal government of Canada enacted the Secure Electronic Signature Regulations (SOR/2005-30), which came into force on February 1 2005. The E-Signature Regs are fairly technical in their definitions and implementation, incorporating digital signature certificates, hash functions and asymmetric encryption employing public and private keys.

What is important in the context of electronic evidence is that when an electronic document is signed using a secure electronic signature, the data in the document are presumed to have been signed by the person identified by the digital signature certificate, in the absence of evidence to the contrary. The use of the regulated signature technology

should enable parties and the courts to determine whether the electronic document was changed after it was electronically signed. This type of technology may be particularly important in the context of laboratory work, where signed electronic records are often submitted to document inventive discovery.

A modern forum

The relevance and importance of electronic evidence regarding both patent prosecution and patent litigation are clear. It is critical that the inventive process is well-documented, that subsequent patent applications are well-supported and that relevant electronic evidence is admissible if allegations of invalidity arise in the context of a patent dispute. The federal and provincial governments of Canada have established the legislative framework that will allow innovators to rely on electronic documents produced during the research and development phase. It will now be up to the Canadian Patent Office and the Canadian courts to provide a modern forum for electronic records as documentary evidence of invention.