BRIDGING TIME: InterPARES and E-DISCOVERY

By Stuart Rennie

Barrister& Solicitor
The InterPARES (International Research on Permanent Authentic Records in Electronic Systems) Project, University of British Columbia
Vancouver, British Columbia, Canada
Stuart_Rennie@telus.net

Writing in 1945, the American inventor and engineer Vannevar Bush envisioned a day when any lawyer would have access to a desk-top electronic device, called the memex which would have at hand legal opinions. The memex would operate as "an enlarged intimate supplement" to the lawyer's memory.[1] Arguably modern computers are Bush's memexes incarnated. The electronically stored information on these computers forms the basis for much of electronic discovery. Current e-discovery presents problems and challenges presented to lawyers and others regarding the process of collecting, preparing, reviewing, and producing electronically stored information for the legal process.[2]

Discovery System Requires Change

Currently, there is general agreement by judges and lawyers in the United States, the United Kingdom and Canada that it takes too long to resolve legal disputes in court and it costs too much time and money. As one judge has observed of discovery generally:

> The system simply cannot continue on the basis that every piece of information is relevant in every case, or that the "one size fits all" approach of Rules can accommodate the needs of the variety of cases that come before the Courts.[3]

While there is no small amount of written commentary about e-discovery from lawyers, judges and other professionals, what is lacking in the debate about e-discovery is a systematic scientific inquiry into electronic records as records. What is an electronic record? How do electronic records operate through their lifecycle from creation and classification to maintenance, use and finally to disposition (destruction or long-term preservation)?

Recent developments in archival science offer a bridge to provide answers to these fundamental questions and to provide solutions to the pressing problems inherent in e-discovery. The InterPARES (International Research on Permanent Authentic Records in Electronic Systems) Project is an international collaborative project which, using archival principles, has conducted comprehensive research and created both the theoretical and methodological knowledge essential to the long-term preservation of authentic digital records. The research included experiments regarding records in interactive, experiential and dynamic digital environments. Case studies were conducted on electronic systems used in the arts, sciences and e-government.

The InterPARES Project has insights and recommendations that can be applied to e-discovery to inform its process and provide answers to its problems.

InterPARES Project

The precursor to the InterPARES Project, *The Preservation of the Integrity of Electronic Records*, was conducted at the University of British Columbia in collaboration with the United States Department of Defense (the "UBC Project").[4] The UBC Project established standards for creating reliable electronic records and maintaining their authenticity during their active and semi-active life. One of the UBC Project products was the DoD Standard 5015.2 for recordkeeping systems.[5] The DoD Standard 5015.2 is now widely used the world over.

The InterPARES Project has developed through three phases. InterPARES 1, building on the UBC Project, was conducted from 1999-2001. It produced conceptual requirements for digital records and their authenticity, methods of selection and preservation, and an intellectual framework for policies and strategies.[6] InterPARES 2 began in 2002 and ended in 2007. It developed theory and practices in order to ensure the reliability, accuracy, and authenticity of electronic records from their creation through to their preservation. This research focused on records created in dynamic, experiential and interactive systems in the course of artistic, scientific and governmental activities.[7] InterPARES 3 was initiated in September 2007 and will continue to August 2012. InterPARES 3, composed of regional, national and multinational teams from around the world, is designed to transform the theory and practice of digital preservation drawn from research to date into concrete action plans for existing bodies of records that are to be kept over the long term by archives and other organizations operating with limited resources.[8]

InterPARES 2 and E-discovery

The theory and practice developed by InterPARES 2 are most applicable to e-discovery. InterPARES 2 has three relevant sets of contributions. The first includes the concepts of accuracy, reliability and authenticity of electronic records. The second is constituted of methods of appraisal and preservation of electronic records. The third is the framework for organizations to develop policies, strategies and standards for the long-term preservation of electronic records.

Accuracy, reliability and authenticity of electronic records

E-discovery is centrally concerned with the accuracy, reliability and authenticity of electronic documents. With Rules of Court procedures established when the legal world was dominated by pen and paper, as a result "documents" still form the basis of legal discovery in the United States, United Kingdom and Commonwealth countries like Canada. In these jurisdictions there are different legal definitions for "document". This has resulted in confusion in e-discovery applications. For lawyers and clients managing cross-border applications, this confusion is compounded.

For example, under federal Tax Court of Canada rules of procedure, "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."[9] Under the provincial law of Canada in British Columbia, "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."[10] Unlike British Columbia, in Ontario provincial law, there is no "extended meaning" to "document" that is of a permanent or semi-permanent character and recorded or stored by means of any device. In Ontario: "document" includes a

sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account, and data and information in electronic form.[11]

In the United States Federal Code of Procedure, "document" is added to "electronically stored information". Both include "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form".[12]

In the United Kingdom, "document" is worded the broadest of all: it "means anything in which information of any description is recorded".[13]

Cross-Border Commercial Litigation Scenario

A commercial litigation scenario illustrates the confusion. Consider a cross-border commercial litigation matter involving two multi-national corporations. One party has business operations in London, England, New York, Vancouver and Toronto. This party has a mixed format business consisting of paper records and an increasing number of electronic records in various formats. An enterprise document and records management system is in use at each regional office. Accounting software and litigation support software are also used. Various websites are maintained for sharing information by all offices of the corporation around the world. The law of each jurisdiction requires business records be created, maintained and retained according to the legislation of each jurisdiction.

Regarding cross-border complex civil litigation, the discovery process raises some basic questions. For the purposes of the Tax Court of Canada, are paper copies of accounting information sufficient for discovery purposes or is the corporate accounting website also required to be reproduced since it contains information "stored using any device"?[14] Do electronic business records from the Vancouver, British Columbia offices include the "metadata," since the definition of "document" in British Columbia has an "extended meaning"?[15] Are the metadata for emails from the New York office discoverable or not—considering recent decisions in the American courts holding that Rule 34(a) of the Federal Rules of Procedure has a general presumption against the production of metadata?[16] For the Ontario office, to ensure that it does not inadvertently disclose privileged information in production for discovery, must the party conduct a page-by-page review of its electronic records, which number in the tens of thousands?[17] For the London office, are third-party expert reports discoverable given the broad definition of "document" in the United Kingdom?[18]

When considering e-discovery, the simple scenario moves quickly to complex matters. The case law interpreting these questions is different for each jurisdiction. To date, there is no consistent legal rule regarding "document" across jurisdictions.

InterPARES 2 Definitions

Relying on rules in different jurisdictions causes confusion, increases costs, expends time and imposes extra administrative burden on parties. An alternative is to adopt InterPARES 2 definitions. InterPARES 2 definitions are broad enough to comply with these various court rules but specific enough for the creator of records to manage its records for its business purposes. The InterPARES 2 approach to electronic records is to assume control of records when records are created. That way, issues regarding records can be identified at the records creation stage. This approach helps in law matters. It assists in identifying issues to be tried at the

early stage of litigation. In the e-discovery literature, identifying all relevant issues to be tried at an early stage in litigation has been found to be an indicator of success.

InterPARES 2 provides consistent definitions derived from archival science that can be used for e-discovery. The defined terms include: “document”, “record”, “accuracy”, “reliability”, “authenticity” and “authentication”.[19] “Document” is information affixed to a medium in a fixed form. Unlike the legal rules of procedure, the InterPARES 2 focus is not on “document” but on “record”. “Record” is any document created, made or received and saved for further action or reference by a physical or corporate person in the course of a practical activity as an instrument and by-product of that activity. Under this analysis, all records are documents, while not all documents are records. Unlike the legal definitions of “document”, the InterPARES 2 conception of a “record” requires information or content, a fixed form and a practical activity that is complete. Unlike the paper document, the “content, form and wholeness of electronic documents are determined conceptually and logically rather than physically”.[20] Focussing on the intellectual production of records, instead of their physical form, goes a long way to providing effective e-discovery that is legally compliant and practical.

“Accuracy” is the degree to which the data in the records are precise, correct, truthful and free of error or distortion. Ensuring accuracy requires the author of these records to exercise control on the processes of creation, transmission, maintenance and preservation of the records. This responsibility for accuracy shifts from the author to the keeper of the records and later, if these records are to be preserved, to the long-term preserver of the records. “Reliability” is the trustworthiness of digital records as statements of fact or as content. Reliability is the responsibility of the author of these records. Reliability can be inferred from the completeness of the record and the controls exercised on the process of creation, including controls exercised on the author (e.g. a nurse cannot issue a diagnosis, only a doctor can). “Authenticity” refers to the fact that the records are what they purport to be and have not been tampered with or otherwise corrupted. Authenticity must be protected whenever records are transmitted across space and time. Over time, the responsibility for authenticity moves from the keeper to the long-term preserver of the records. Its assessment is based on the identity and integrity of the record. “Authentication” is a declaration of authenticity, resulting either from the insertion or the addition of elements or statements to the records in question. The rules governing authentication are established by legislation, case law or rules of procedure.

InterPARES 2 links these definitions in a chain. This ensures electronic records conform to these definitions. In turn, this ensures that electronic records, from their inception to their disposal or preservation are accurate, reliable and authentic.

In addition to setting an intellectual framework for the definition of “record”, InterPARES 2 has laid down guidelines for creators who make and maintain electronic records. These guidelines recommend that:

- hardware, software and file formats be selected that offer the best hope for ensuring that digital materials will remain easily accessible over time;
- digital materials maintained as records are stable and fixed both in their content and in their form;
- digital materials be properly identified, not just by naming files but by metadata;
- digital materials carry information that will help verify their integrity by integrity metadata;
- organize digital materials into logical groupings, following a written records classification plan and retention schedule;

- authentication techniques be used that foster the maintenance and preservation of digital materials when digital materials are transmitted across space or time;
- digital materials be protected from unauthorized action using physical security, access privileges and blocks on modifying records once filed pursuant to a classification plan;
- digital materials be protected from accidental loss and corruption using daily backups;
- steps be taken to prevent hardware and software obsolescence by upgrading and migrating to new technology and retaining relevant documentation for long-term preservation; and
- issues surrounding long-term preservation be considered at the record creation stage and for that small number of records identified for long-term preservation using a trusted custodian.[21]

Identity Metadata and Integrity Metadata

Applying the proper identification of electronic records using the InterPARES 2 guidelines regarding metadata greatly assists in preserving the chain of custody. The chain of custody proves the integrity of the electronic records as evidence.

There is consensus in the legal literature that metadata is one of the most difficult matters to manage in e-discovery. Legislation has yet to comprehensively define metadata. Metadata is a part of the integrity of evidence. Some recent legislation has specifically addressed integrity, not of records, but of the electronic records system. For example, section 31.3 of the *Canada Evidence Act* lists the legal presumptions to prove the integrity of the electronic records system.[22]

Metadata issues are expressly addressed in the legal "best practices" models set out in the Sedona Principles and the Sedona Canada Principles. Principle 12 of the Sedona Principles recommends that production should be made in the form in which the information is ordinarily maintained, including providing reasonably accessible metadata permitting the receiving party the same ability to access, search, and display the information as the producing party.[23] Principle 8 of the Sedona Canada Principles recommends that, as early as possible in the litigation, parties should agree on the format in which electronically stored information will be produced.[24]

InterPARES 2 defines metadata as the properties or attributes conveying the identity of a digital object that is to be kept as a record and the fact that it is complete and unaltered in all essential respects.[25] The fields of identity metadata include: author, matter, form, date and classification code.[26] Identity metadata are important because retrieval is always based on identity metadata. Also, if a party does not know the record's identity as expressed in the identity metadata, how does the party know that the record is intact, that it has integrity, that it has not been doctored with?

While identity metadata distinguish between electronic records, integrity metadata lets a party infer that the records are the same as when they were created. The fields of integrity metadata include: names of the handling person/office, technical changes to the materials, access restriction/privileges code, vital record code (degree of importance of the record) and planned disposition (removal from the live system to storage outside the system, transfer to the care of a trusted custodian or scheduled deletion).[27]

The InterPARES 2 integrity metadata guidelines incorporate the attributes necessary to prove the integrity of electronic records as evidence. Following the InterPARES 2 integrity metadata guidelines permits a party to

prove it can produce reasonably accessible metadata permitting the receiving party the same ability to access, search, and display the information as the producing party (Principle 12 of the Sedona Principles). As well, InterPARES 2 allows a party to agree on the format in which electronically stored information will be produced (Principle 8 of the Sedona Canada Principles) and prove the integrity of is electronic records system (section 31.4 of the *Canada Evidence Act*).

Regarding planned disposition, the InterPARES 2 integrity metadata guidelines provide for an orderly, routine and businesslike disposition of electronic records in the ordinary and usual course of business. That way routine disposal of electronic records not part of the discovery process can continue so the organization can be legally compliant and conduct its business as usual.

Authentication of Documentary Evidence Using Diplomatic Principles

InterPares 2 performed research into authenticating electronic records and entities using diplomatic analyses. Diplomatics is the "discipline which studies the genesis, forms and transmission of archival documents, and their relationship with the facts represented in them and with their creator, in order to identify, evaluate, and communicate their true nature."[28]

InterPARES 2 conducted over two dozen diplomatic case studies. These diplomatic analyses ranged from examining museum web exhibits and assessing e-revenue systems to reviewing survey records from the planet Mars. Most relevant to e-discovery is the diplomatic analysis of the computerization of Alsace-Moselle's land registry in France.[29] This computerization project digitized paper land registry records from 1891. It also computerized the system of recording real estate transactions, validating these transactions by a judicial officer and transmitting registry information. InterPARES 2 findings were that this computerized land registry met all the requirements of a record. There were strict procedural and documentary controls in place. This ensured that records are reliable and the controls on them ensured the authenticity of the records over time.[30]

Applied to e-discovery, InterPARES 2 diplomatic analysis can be used in requests for admissions to authenticate documents. By doing so, diplomatics applied to e-discovery is a new tool for lawyers to use. Diplomatic analyses can be used in pre-discovery discussions between counsel. It can be used also to limit the scope of production and discovery. It can assist in determining admissibility of Internet information. It can work to resolve evidentiary issues, including the application of the best evidence rule.

Methods of appraisal and preservation

Appraisal and preservation, long key functions for archivists for centuries, are also key features for e-discovery.[31] Appraisal assesses the continuing value of the records, assembles evidence for the presumption of their authenticity and identifies the digital components or objects that need to be stored and reproduced in order to ensure the preservation of authentic records.[32]

Regarding preservation, three InterPARES 2 findings are applicable. [33] First, it is not possible to preserve a digital record since it is only possible to preserve the ability to reproduce the record. Second, the intellectual and physical components of a digital record do not necessarily coincide since a digital component is distinct from an element of documentary form, so that, for instance, the content of a record may include both text

contained in a word processing file and a table generated by spreadsheet software. Third, preservation begins at creation of the record and must be thoroughly documented as a primary means for protecting and assessing authenticity over the long term. Since preservation begins at creation, responsibility for this thorough documentation rests with both the creator and the preserver. The research findings from InterPARES 2 are that "too many records creators are still neglecting the long-term preservation of their digital files, whether they be static or dynamic, evidential or experiential, historically significant or interactive".[34]

The InterPARES 2 focus on what to preserve at the creation stage of the record life cycle is consistent with the e-discovery principle of only producing and disclosing electronic records that fulfill legal and business values relevant to litigation.

Historically, in the British common law world, there is an open door policy to disclosure. In the United Kingdom, Canada and other Commonwealth countries, this arose as a result of the 1882 *Peruvian Guano* Rule where the English Court of Appeal held that there is a legal duty to: "disclose every relevant document that reasonably contains information which may either directly or indirectly enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary."[35] Since 1882, rules of court have embodied the *Peruvian Guano* Rule. The problems in part posed by e-discovery of electronic records are causing the legal profession and the judiciary to rethink the *Peruvian Guano* "disclose everything" ethos.

Courts are slowly coming to appreciate the fact, confirmed by InterPARES 2 research, that electronic records are different from paper documents, and to appreciate that it is the thorough documentation of the electronic record from its creation that attests to its authenticity for legal purposes. This is so because, again, it is not possible to preserve an electronic record but only the ability to reproduce it. Thus, evidence of its authenticity is always circumstantial, always an inference. A weak link in the chain of custody/preservation means that we cannot trust the record and the only way to verify its authenticity is to find an authentic copy of it somewhere else. This also means that, once the creator no longer uses the record in the usual and ordinary course of business, trust in the record begins to weaken, so the record should be put in the hands of a neutral third party, the designated custodian, who has no stake in the content of the record.

In InterPARES 2, since it is the creator that controls records creation, the responsibility for this thorough documentation rests with the creator as well as the preserver. Cooperation between the creator and preserver are implied. For instance, this InterPARES 2 principle is inconsistent with the traditional legal rule on costs. Generally, each party in litigation bears its own costs to organize its records, prepare lists of documents and disclose them to the other party in litigation. Costs are paid at the end of the litigation.[36] The emerging trend in e-discovery best practices is to provide for cost-shifting and cooperation between parties. Both the Sedona Principles and Sedona Canada Principles recognize that costs of preserving and producing electronically stored information may need to be shared. They recommend a proportionality standard be applied. The proportionality standard is that disclosure should be proportionate, taking into account the importance and complexity of litigation, the relevance of the available electronically stored information, its importance to the court's adjudication in a given case and the costs, burden and delay that may be imposed on the parties to manage electronically stored information.[37]

This best practice cost-shifting model is in opposition to traditional modes of lawyering where lawyers are zealous advocates for their clients and have conduct of the trial, while the litigants decide, after consulting their legal counsel, what is proportionate in any given legal claim. In the heated debate in British Columbia

surrounding proposals to change the 2008 Proposed New Rules of Civil Procedure of the British Columbia Supreme Court to include, among other things, the proportionality standard, one legal stakeholder organization articulated its opposition to proportionality this way:

> The mantra that the judge is to invoke is whether the procedures to be followed in the case are 'proportionate.' In other words, if the judge, without evidence and without a real understanding of the case, decides that she is going to limit the parties' ability to discovery, to the number of expert witnesses, to the matters that expert evidence may be given on, to a jury trial and so on, that is final.[38]

In Canada, rules of court are being amended in Ontario, Alberta and British Columbia to incorporate proportionality and other changes, such as having the court actively involved in the management of the litigation. The United States Rules of Federal Procedure already incorporate principles of proportionality. The tension between proportionality and lawyer conduct of litigation is an ongoing one and not likely to be resolved anytime soon. As the volume and type of electronic records created by parties increases, and if proportionality is mandated by legislation more broadly, the IntePARES 2 model of focusing on thorough documentation of records chosen to be created, and cooperation between the record creators and preservers, may be a preferred model.

Benchmarks: Presumption Of Authenticity

InterPARES 2 provides a concrete benchmark where authenticity of electronic records can be presumed. Meeting this benchmark permits the inference by the preserver that the records are authentic as a result of the manner in which the records have been created, handled and maintained by the creator. This benchmark has these components which must be met:

- record attributes are stated (such as name of record author) and linked to the record (identity and integrity metadata);
- the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation and destruction of records;
- the creator has established and effectively implemented procedures to prevent, discover and correct loss or corruption of records;
- the creator has established and effectively implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change;
- the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator;
- if authentication is required by the juridical system or the needs of the organization, the creator has established specific rules regarding which records must be authenticated, by whom, and the means of authentication;
- if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative; and
- if there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the electronic system, the creator has established and effectively implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records. [39]

This InterPARES 2 presumption of authenticity benchmark is consistent with the existing case law and legislation regarding authentication. For example, for destruction of electronic records to qualify as spoliation

warranting court sanctions, it is required that fraud or some intentional act occurs to improperly destroy documentary evidence.[40] A claim of spoliation can be rebutted by evidence from the implementation of the InterPARES 2 benchmark that access privileges to the electronic records were in place to prevent improper destruction, that procedures were followed to prevent loss, corruption, deterioration or accidental destruction of electronic records, that documentary forms of the electronic records complied with rules of an applicable juridical system, and that procedures were followed to control copies and identify which electronic record is authoritative and to be relied upon as evidence.

Baseline: Production Of Authentic Electronic Record Copies

Where the InterPARES 2 presumption of authenticity benchmark establishes the record's identity and lays a foundation for demonstrating its integrity,[41] the InterPARES 2 baseline requirement for the production of authentic electronic record copies is a feature to manage preservation. This baseline describes the minimum conditions necessary to enable the preserver to attest to the authenticity of copies of inactive electronic records.[42] There are three minimum baseline conditions. First, there are controls over records transfer, maintenance, and reproduction to guarantee the records' identity and integrity. Second, there is documentation of the reproduction process and its effects. Third, there is archival description of the fonds (whole of the documents collected) containing the electronic records. Archival description functions as a collective authentication of the aggregation of the records, which are shown in their documentary context, in their interrelationships with all the other records of the same creator and with the functions and activities of the creator.

To date, the issue of duplicate copies in e-discovery has received scant judicial attention. There is a preponderance of electronic duplicates in both the business and legal worlds. But there is little legal authority whether or not drafts of documents—be they in paper or digital form-- are discoverable when the final document is discoverable. One Canadian court has devised this test: "The test must be whether the draft is also relevant and material, which must in turn depend on whether some relevant inference can be drawn from the differences between the draft and the final version."[43]

The InterPARES 2 baseline can assist litigators by providing evidence whether or not a draft document is relevant. The baseline can help to determine if electronic records are material to the case at bar. The baseline can provide information to determine if the evidence is not too remote to the litigation issues. Finally, the baseline can be used to discover if relevant inferences can be drawn from the differences between draft and final versions of electronic records.

Policies for the long-term preservation of electronic records

A major finding of the InterPARES 2 research is that, to preserve trustworthy electronic records that are proven to be accurate, reliable and authentic, records creators must create them in such a way that it is possible to maintain and preserve them. Further, this process requires a cooperative relationship between a records creator and its designated preserver and this must begin at the time the records are created.[44]

InterPARES 2 has produced a set of principles for use by records creators and corresponding principles for use by records preservers. The principles for records creators can be used to bring to bear key issues for creators to consider regarding the creation, maintenance and use of electronic records within any organization. The principles for records preservers are intended for persons with knowledge of records who are responsible for

developing policies and strategies within their organizations where the goal of the organization is the long-term preservation electronic records.

To illustrate, an InterPARES 2 record creator principle that can be applied to the e-discovery process is the following: record creation and maintenance requirements should be formulated in terms of the purposes the records are to fulfil, rather than in terms of the available or chosen record-making or recordkeeping technologies.[45] Overreliance on recordkeeping technologies is an example of the tail wagging the dog. Technologies change frequently as they are upgraded.[46] Technologies contain commercial rights and copyright considerations that may complicate matters. For these reasons, it is incumbent on organizations to get their records house in order in using these technologies selectively.

As a further example, another InterPARES 2 record creator principle can be used in e-discovery. This principle is that a trusted custodian should be designated as the preserver of the creator's records.[47] A trusted custodian is an individual who has formal education and experience in records and archives administration. The trusted custodian acts as a neutral third party. As a third party, the trusted custodian has no reason to alter records in its custody and will not allow anyone to alter records, accidentally or on purpose. The trusted custodian must establish a trusted preservation system capable of ensuring that accurate and authentic copies of the creator's records are acquired and preserved. There is a role for the trusted custodian in discovery.

A recent survey of experienced American trial lawyers identified as pressing problems: early identification of issues must be made to decrease costs, (especially when large number of electronic records are involved or claims are frivolous), discovery must be limited (especially since e-discovery increases the costs of litigation) and judges should have a more active role in discovery (including ordering alternative dispute resolution early in the litigation process).[48]

In effect, the trusted custodian operates as an expert, accepted by both parties in litigation. The trusted custodian can have a role in pre-discovery discussions between counsel. As a records expert, the trusted custodian can help to winnow out frivolous and vexatious claims. In pre-trial conferences and judicial management conferences, the trusted custodian can also act as a friend of the court and assist and instruct the judge, lawyers and parties on records matters in general and matters specific to the electronic records at issue in the litigation. The trusted custodian could also act as mediator in disputes over records.

In conclusion, InterPARES Project research on the accuracy, reliability and authenticity of electronic records, methods of appraisal and preservation, and policies for the long-term preservation of electronic records can support lawyers and judges in the e-discovery process. InterPARES can assist to bridge the time between when electronic records are created and when they are needed again in the litigation process.

---

[1] Vannevar Bush. "As We May Think" The Atlantic (July 1945) < http://www.theatlantic.com/doc/194507/bush/>.

[2] "Electronic Discovery ("E-Discovery")" defined in The Sedona Conference, *The Sedona Glossary: For E-Discovery And Digital Information* Management (3rd ed.) (December 2007), <http://www.thesedonaconference.org/>.

[3] American College Of Trial Lawyers and The Institute For The Advancement Of The American Legal System. *Final Report On The Joint Project Of The American College Of Trial Lawyers Task Force On Discovery And The Institute For The Advancement Of The American Legal System* (Revised April 15, 2009) at page 25,

<http://www.actl.com/AM/Template.cfm?Section=Home&template=/CM/ContentDisplay.cfm&ContentID=4008>[*American Discovery Report*].

[4] *The Preservation of the Integrity of Electronic Records*. Luciana Duranti Principal Investigator (1997), <http://www.interpares.org/UBCProject/index.htm>. See also Luciana Duranti, Terry Eastwood and Heather MacNeil, *Preservation of the Integrity of Electronic Records* (Dordrecht: Kluwer Academic Publishers Group, 2002).

[5] Department of Defense Assistant Secretary Of Defense For Command, Control, Communications And Intelligence. *Design Criteria Standard For Electronic Records Management Software Applications*. (2002), <http://www.interpares.org/display_file.cfm?doc=DoD_50152.pdf>.

[6] *The Long-term Preservation of Authentic Electronic Records: The Findings of The InterPARES Project.* Luciana Duranti ed. (San Miniato: Archilab, 2005), <http://www.interpares.org/book/index.cfm>.

[7] *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*. Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008), <http://www.interpares.org/ip2/book.cfm>.

[8] See http://www.interpares.org/ip3/ip3_index.cfm.

[9] Section 78(1) of the Tax Court of Canada Rules (General Procedure) (SOR/90-688a) of the *Tax Court of Canada Act* (R.S., 1985, c. T-2).

[10] Rule 1(8) of the Supreme Court Rules (B.C. Reg. 221/90) of the *Court Rules Act,* R.S.B.C. 1996, c. 80.

[11] Rule 30.01(1)(a) in Rules Of Civil Procedure under the *Courts of Justice Act*, R.R.O. 1990, Regulation 194.

[12] Rule 34(A), Federal Rules Of Civil Procedure.

[13] Part 31.4 Disclosure And Inspection Of Documents in Rules and Practice Directions (49th update April 6, 2009) in *Civil Procedure Rules: Practice Directions, Pre-Action Protocols And Forms*. (2nd (consolidated) ed. 2005) (3v.) (as amended).

[14] *ITV Technologies Inc. v. WIC Television Ltd.*, 2003 FC 1056 (CanLII), where the Federal Court of Canada held that "the original is found on the Internet and provides better evidence than a print copy. The Court was able to see the documents as they existed on the Internet, and could witness such features as hyperlinking and interactive streaming that could not have been realistically reproduced on paper." (at para. 13), <http://www.canlii.org/en/ca/fct/doc/2003/2003fc1056/2003fc1056.html>.

[15] *Desgagne v. Yuen et al*, 2006 BCSC 955 (CanLII). The Supreme Court of British Columbia held that the metadata "does not fit the ordinary or intuitive concept of a document, electronic or otherwise... That data is not something created by the user, but it is based on what the user does with her software. It is not something that has content in the same sense as a document file generated by the user, for example, a word processing document or spreadsheet. Nor is it something which is printed out or emailed in the ordinary course. The assistance of an expert is required to generate the metadata report. In spite of this, it appears clear that the metadata is 'information recorded or stored by means of [a] device' and is therefore a document under Rule 1(8)." (at para. 29), < http://www.canlii.org/en/bc/bcsc/doc/2006/2006bcsc955/2006bcsc955.html>.

[16] *Williams v. Sprint/United Management Co. ,* 230 F.R.D. 640, 646-57 (D. Kan. 2005) relying on the Principles 12 and Comment 12.a. of the 2005 Sedona Principles, the Court found "emerging standards of electronic discovery appear to articulate a general presumption against the production of metadata, but provide a clear caveat when the producing party is aware or should be reasonably aware that particular metadata is relevant to the dispute."(page 13), < http://www.electronicdiscoveryblog.com/cases/williams.pdf>.

[17] *Air Canada v. WestJet Airlines Ltd.* 2006 CanLII 14966 (ON S.C.). The Ontario Superior Court of Justice refused to permit a party to provide electronic disclosure of some 75,000 documents without manual review. While not ordering a page-by-page manual review,

the Court required the party to review different categories of documents with different levels of review such that the diligent search requirements of the Ontario *Rules of Civil Procedure* were met. The Court refused to make an order confirming that if privileged documents are inadvertently produced by the party, such production will not constitute waiver of privilege or admission of relevance since solicitor and client privilege is so fundamental to the justice system in Canada that it should not "readily be sacrificed to the interests of expediency or economics." (at para. 15), <http://www.canlii.org/en/on/onsc/doc/2006/2006canlii14966/2006canlii14966.html>.

[18] *Smithkline Beecham Plc v Generics (UK) Ltd.* [2003] EWCA Civ 1109. The Court of Appeal upheld the lower court and refused to order disclosure of third-party records in the interests of public justice: "First, the subject matter of the documents is confidential. Second, they originate with third parties. Third, they are of peripheral relevance at best to explain the issues in the action. Fourthly, they are not part of the material which is needed to explain the judgment. Fifthly, they are not needed to explain the judgment of the Court of Appeal which does not refer to them. Sixthly, they cannot be explained without considerable context or speculation exposing their makers or the employers of their makers to further requests for further information." (at para. 30), <http://www.hrothgar.co.uk/YAWS/reps/03a1109.htm>

[19] John Roeder, Philip Eppard, William Underwood and Tracey P. Lauriault, "Part Three—Authenticity, Reliability and Accuracy of Digital Records in the Artistic, Scientific and Governmental Sectors: Domain 2 Task Force Report," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008) at page 43, <http://www.interpares.org/display_file.cfm?doc=ip2_book_part_3_domain2_task_force.pdf> [*Creator Guidelines*].

[20] Luciana Duranti and Kenneth Thibodeau, "The Concept of Record in Interactive, Experiential and Dynamic Environments: the view of InterPARES", *Archival Science* (2006) 6:13-68 at 28.

[21] *Creator Guidelines* at pages 44-52.

[22] Section 31.1 states, that in the absence of evidence to the contrary, the integrity of an electronic documents system may be proven in one or more of three ways. First, the integrity of the electronic records system is proved by evidence that the computer system was operating properly. Second, the integrity of the electronic records system is proven if the electronic record was recorded or stored by a party who is adverse in interest to the party seeking to introduce it. Third, the integrity of the electronic records system is proven 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 and who did not record or store it under the control of the party seeking to introduce it. This creates a presumption of reliability for the business records of a person who is not a party to the legal proceeding, where the person claiming the record as evidence did not control the making of the record. Section 31.1 was considered without direction in *R. v Bellingham*, 2002 ABPC 41 (CanLII), <http://www.canlii.org/en/ab/abpc/doc/2002/2002abpc41/2002abpc41.html>.

[23] The Sedona Conference, *The Sedona Principles: Second Edition Best Practices Recommendations & Principles for Addressing Electronic Document Production* (June 2007), <http://www.thesedonaconference.org/>[*Sedona Principles*].

[24] The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery* (January 2008), <http://www.thesedonaconference.org/>[*Sedona Canada Principles*].

[25] *Creator Guidelines* at page 47.

[26] *Ibid.*

[27] *Supra* at page 48.

[28] InterPARES 2 Project, "The InterPARES 2 Project Glossary," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008) at page 17, <http://www.interpares.org/display_file.cfm?doc=ip2_book_glossary.pdf>.

[29] InterPARES 2 Project, "Diplomatic Analysis Case Study 18: Computerization of Alsace-Moselle's Land Registry" by Jennifer Douglas in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008).

[30] *Supra* at page 7.

[31] Yvette Hackett, "Part Four—Methods of Appraisal and Preservation: Domain 3 Task Force Report," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records,* Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008), <http://www.interpares.org/display_file.cfm?doc=ip2_book_part_4_domain3_task_force.pdf>[*Appraisal and Preservation*].

[32] Luciana Duranti (2001), "International Research on Permanent Authentic Records in Electronic Systems (InterPARES): Experiential, Interactive and Dynamic Records," SSHRC MCRI InterPARES 2 Project Proposal, 412-2001, 1.1-12, <http://www.interpares.org/display_file.cfm?doc=ip2_detailed_proposal.pdf.>.

[33] *Appraisal and Preservation* at page 4.

[34] *Supra* at page 13.

[35] *Compagnie Financiére du Pacificque v. Peruvian Guano Co.* (1882), 11 Q.B.D. 55 (C.A.) (Brett L.J. at page 62). The Supreme Court of Canada has confirmed the "fundamental importance of discovery" of the *Peruvian Guano* Rule, see *Hunt v. T&N PLC* 1993 CanLII 43 (S.C.C.) at page 46, <http://www.canlii.org/en/ca/scc/doc/1993/1993canlii43/1993canlii43.html>.

[36] *Barker v. Barker*, 2007 CanLII 13700 (ON S.C.) at para. 14. The Ontario Superior Court of Justice ordered plaintiffs to pay one-third of defendants' cost to convert old paper records to electronic form because of the substantial continuing benefits to all parties and the court that these "benefits will extend beyond the process of discovery" (at para. 15), <http://www.canlii.org/en/on/onsc/doc/2007/2007canlii13700/2007canlii13700.html>.

[37] Principle 2 in each of the *Sedona Principles* and *Sedona Canada Principles*.

[38] Trial Lawyers Association Of British Columbia, " Trial Lawyers Association Of British Columbia Response to the BC Justice Review Task Force Talking Points on Proposed Rules of Civil Procedure of the British Columbia Supreme Court Questions and Answers dated September 15, 2008" at page 5, < http://www.tlabc.org/BC/>.

[39] *Appraisal and Preservation* at pages 51-56.

[40] In Canada, spoliation requires that relevant documents in pending legal proceedings were destroyed, where the destruction of documents was an intentional act indicative of fraud, or an intention to suppress the truth per *Holland v. Marshall*, 2008 BCCA 468 (CanLII), <http://www.canlii.org/en/bc/bcca/doc/2008/2008bcca468/2008bcca468.html>. See also, British Columbia Law Institute, Report on Spoliation of Evidence (Number 34) (November 1, 2004), <http://www.bcli.org/bclrg/publications/34-report-spoliation-evidence>.

[41] *Appraisal and Preservation* at page 51.

[42] *Supra* at pages 57-59.

[43] *Turkawski v. 738675 Alberta Ltd.* 2005 ABQB 423 (CanLII) at para. 52, <http://www.canlii.org/en/ab/abqb/doc/2005/2005abqb423/2005abqb423.html>.

[44] Luciana Duranti, Jim Suderman and Malcolm Todd, "Appendix 19: A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti

and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008) at page 1, <http://www.interpares.org/display_file.cfm?doc=ip2_book_appendix_19.pdf>[*Preservation Policies*].

[45] Creator Principle 3 (C3) in *Preservation Policies* at page 6.

[46] *JDS Uniphase Inc. v. Metconnex Canada Inc.*, 2006 CanLII 34432 (ON S.C.) Regarding cost-splitting, dispute was as to the functionality made by each party of SUMMATION software for search, retrieval and metadata for discovery purposes. Parties initially made agreement for this use but in processing the software increased costs arose.
< http://www.canlii.org/en/on/onsc/doc/2006/2006canlii34432/2006canlii34432.html>.

[47] Creator Principle 8 (C8) in *Preservation Policies* at page 10.

[48] *American Discovery Report* at page 2, <http://www.actl.com/AM/Template.cfm?Section=Home&template=/CM/ContentDisplay.cfm&ContentID=4008>. See also more information about the survey in *Interim Report & 2008 Litigation Survey of the Fellows of the American College of Trial Lawyers* (September 9, 2008) at page 2, <http://www.du.edu/legalinstitute/pubs/Interim%20Report%20Final%20for%20web1.pdf>.