Canadian Journal of Law and Technology

Volume 8 | Number 2 Article 1

10-1-2010

The Admissibility of Electronic Business Records

Ken Chasse

The Admissibility of Electronic Business Records

Ken Chasse*

INTRODUCTION

The business record provisions of the Evidence Acts determine a record's admissibility by evidence of its history, which must be the product of "the usual and ordinary course of business" (or comparable "business activity" wording). The electronic record provisions determine a record's admissibility by the, "integrity of the electronic records system in which it is recorded or stored." The difference is, records management (RM) based on "paper records concepts" versus "electronic records systems concepts." The former is subjective — each business determines its own "usual and ordinary course of business"; the latter, objective — in accordance with authoritative standards of RM. Because of the many new laws that demand and depend upon records, electronic RM is now a matter of "legal compliance" and not merely good business practice. The business record provisions were enacted when: (1) electronic records came from stand-alone mainframe computers and not complex computer networks; (2) most of the present methods of, and reasons for making false records and damaging RM systems did not exist; for example, paper record systems cannot be damaged "remotely," nor by software failures and error rates; and, (3) objective, authoritatively recognized national and international standards of electronic RM did not exist. The "usual and ordinary course of business" test allows every business to choose its own principles and practices of RM. Therefore it is now too subjective and vague to provide sufficient protection against the use of unreliable records as evidence. The objective, standards-based "system integrity" test must therefore become the sole test of admissibility and "weight." Or, the business record provisions be reinterpreted so as to judge RM systems and not individual pieces of paper — an alteration perhaps more appropriately left to the legislature. The American case law is used as a comparison. And common electronic RM practices and defects are referred to because the admissibility and "weight" of electronic business records should be interdisciplinary determinations. That is what the "system integrity" of electronic RM requires. A list of points made appears immediately before the Appendices.

* Ken Chasse, member of the Law Society of Upper Canada (Ontario), and of the Law Society of British Columbia, kchasse@fixy.org.

I. THE PROBLEM — NO ADEQUATE ADMISSIBILITY TEST AND ITS "DISCLOSURE" CONSEQUENCES

(a) "System integrity" versus "the usual and ordinary course of business"

The electronic records provisions[1] of the Evidence Acts put forward an "electronic records system integrity test." It will be very effective when it has case law providing definition, interpretation, and examples for its application. In contrast, the "usual and ordinary course of business" test of the business record provisions is now too weak to adequately guard against the use of unreliable electronic records as evidence. Its "business activity" wording is an adaptation of an American "model Act" wording enacted in Canada in 1969.[2] It is inadequate for judging the reliability of the records produced by a since-created sophisticated technology, far beyond the 1969 stand-alone mainframe computers limited to the batch-processing

---

1 "Electronic records" means electronically-produced records, which includes almost all records today. And "electronic" includes "optical" which refers to optical systems, which operate on photons of light instead of flows of electrons. For example, the Ontario *Evidence Act* (OEA), R.S.O. 1990, c. E.23, s. 34.1(1) states: "'Electronic record' means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device, and includes a display, printout or other output of that data, other than a printout referred to in subsection (6);"Section 34.1(6) OEA provides for the "relied-upon printout." See the references to the "relied-upon printout" in footnotes 35 and 134 *infra*, and accompanying text. "Data" is defined in the same section as: "representations, in any form, of information or concepts." The electronic record provisions of the *Canada Evidence Act* (CEA) R.S.C. 1985, c. C-5, are ss. 31.1 to 31.8. They are reproduced in the table in Appendix C, along with those of the OEA, s. 34.1, the *Alberta Evidence Act* (AEA), R.S.A. 2000, c. A-18, ss. 41.1 to 41.8, and the Nova Scotia *Evidence Act* (NSEA), R.S.N.S. 1989, c. 154, ss. 23A–23G. The *Uniform Evidence Act* (UEEA), being a model Act produced by the Uniform Law Conference of Canada is produced at the end of the table. It is the model Act used to draft the electronic records provisions of these Evidence Acts. That is why they are so very similar across Canada.

2 For example, s. 30 of the *Canada Evidence Act* (CEA) was enacted in 1969 (as s. 29A). It, and its provincial counterparts were a reaction to the decision of the House of Lords in, *Myers v. Director of Public Prosecutions* (1964), [1965] A.C. 1001, [1964] 2 All E.R. 881, 48 Cr. App. R. 348 (U.K. H.L.) [*Myers*]. It held that: (1) the common law hearsay exception for business records was not able to admit an assembly line motor vehicle registration record because its absent author couldn't be proved to be dead; and, (2) Parliament would have to legislate a solution. The Supreme Court of Canada disagreed, simplifying and extending the common law business records exception to the hearsay rule in Canada: *Ares v. Venner*, [1970] S.C.R. 608, 12 C.R.N.S. 349, 14 D.L.R. (3d) 4 (S.C.C.) [*Ares*]. (See also note 21, *infra.)* Between these dates, the present "business record provisions" were added to the Evidence Acts. The "usual and ordinary course of business," test, and the "circumstances of the making" test in the business record provisions both came from the *Uniform Evidence Act of 1953*, which was a "model Act" and not legislation. Section 63(13) used the phrase, "regular course of business." And therefore Rule 803(6) of the U.S. Federal Rules of Evidence uses the phrase, "in the course of a regularly conducted business activity." I refer to these tests collectively as "'business activity' tests of admissibility."

of records.

(b) RM (Records Management) Based Upon "Records Concepts," and Now "Systems Concepts"

In 1969 the following did not yet exist: word-processing, the personal computer, laptops, the Internet, email, online services, computer networks, and all of the many devices upon which electronic data is stored today. Electronic technology was limited to functions that merely speeded-up the procedures of traditional "paper-original" RM. Records were still paper-based or microfilm-based documents. Electronic technology had not yet removed RM from its "records concept" foundation. It hadn't yet changed the fact that the reliability of a record is dependent upon its own history and not that of the record system it comes from. Electronic technology has given RM a fundamentally different foundation. The integrity of an electronically-produced record is dependent upon the integrity of the electronic records system it comes from. A record is now a flow of electrons (or photons of light in an optical system) and not a piece of paper or microfilm. By separating data (information) from such "media of storage," record integrity and reliability become "systems based." And therefore, so must admissibility. For that reason, the electronic records provisions of the Evidence Acts have a "system integrity" rule of admissibility.[3] And therefore those jurisdictions having only a business record provision, such as British Columbia, Newfoundland and Labrador, and U.S. Federal Rule of Evidence 803(6) (FRE 803(6)), will have to give those provisions a "system integrity" interpretation if they are to provide adequate protection against the use of unreliable records as evidence. But their "business activity" type of admissibility rule is a subjective test that allows any poor quality records system to produce admissible records if such records are the product of the usual and ordinary course of "business activity." "Business activity" can no longer provide sufficient protection against unreliable records being used as evidence, if it ever could. But their "circumstances of the making of the record" subsections can.[4]

---

3 Only the Evidence Acts of British Columbia and Newfoundland and Labrador do not yet contain electronic record provisions. The B.C. *Evidence Act* does contain a business record provision, but not that of Newfoundland and Labrador, or Alberta. Therefore the Evidence Acts (or comparable legislation) of 12 of Canada's 14 jurisdictions contain electronic records provisions, and 12 of them contain business record provisions. The business record exception to the hearsay rule at common law can be used with or without a business record provision. Its admissibility test uses the words, "in the routine of business," which provides the historical base of the "business activity" type of business record hearsay exception used in the Evidence Acts today.

4 For example, s. 30(6) CEA links the words, "the circumstances in which the information contained in the record was written, recorded, stored or reproduced," with its opening words, "For the purpose of determining whether any provision of this section applies." Therefore such "circumstances" of any record system can deny its records admissibility. Such "circumstances" can be measured by and be accountable to authoritative standards of electronic records management. That provides good protection against "bad" electronic RM, and expressly makes relevant in interpreting, "the usual and ordinary course of business," the features of "good" electronic RM. However, this use of subsection 30(6) could be made clearer and stronger if its wording expressly

In contrast to the "business activity" type of admissibility test, the word "system" enables the "system integrity test" to be sufficiently flexible to cope with every change in electronic technology applied to RM. The word "integrity" gives it the objectivity and stability inherent in being measurable by and accountable to national and international standards of electronic records management. That is why the electronic records provisions expressly invite the use of standards in determining admissibility.[5] As a result, "system integrity" is a very good test for determining admissibility.

But there are important questions to answer. For example, is "a system" the whole of an organization's electronic RM system? Or are the various departments such as, imaging, payroll, and travel and accommodation expenses each "a system"? Does it include the RM systems of all the branch offices, and does it also depend upon how interdependent they are, or their command structure as to how many chief records managers there are? At what point do corporate "mergers and acquisitions" meld to produce one RM system? Is a breathalyzer machine an electronic RM system that produces expert opinion evidence? It does, and for more than just the fact that its software is the product of expert opinions. The relatively simple software of a typical breathalyzer machine has about 54,000 lines of code having an average error rate of 2.5%, meaning 1,350 lines are vulnerable to error.[6] The more sophisticated software can make discretionary "choice" decisions. Should there be an "expert evidence" voir dire conducted for every printout? And how to prove "integrity," and what is it in regard to electronic RM? Does the error rate of the software of a RM system determine its "system integrity"?

(c) Disclosure and Admissibility Are Interdependent

And how does one get "disclosure and discovery" of that if it isn't in the police "investigative file"?[7] Disclosure and admissibility are so intimately interdepen-

---

made it an "inclusionary" rule and not merely an "exclusionary" rule as it is now. A similar subsection exists in the business record provisions of the provincial and territorial Evidence Acts, but they expressly apply only to "weight" and not to admissibility. That would have to be amended if they were to provide protection against the use of unreliable electronic records as evidence.

5 See for example, s. 31.5 CEA, and s. 34.1(8) OEA. See Appendix C because it contains the electronic records provisions of the CEA, OEA, the *Alberta Evidence Act* (AEA), and the NSEA. For the National Standards of Canada, see *infra* notes 40, 53, 78, and 165, and accompanying text.

6 See notes 129–132 and accompanying text in, Ken Chasse, "Electronic Discovery in the Criminal Court System" (2010) 14 Canadian Criminal Law Review 111 at 156-157.

7 As to the disclosure obligations upon the Crown prosecutor in relation to the "investigative file," see: *R. v. McNeil*, [2009] S.C.J. No. 3, [2009] 1 S.C.R. 66, ¶42; *R. v. Shearing*, [2002] 3 S.C.R. 33, 165 C.C.C. (3d) 225, 2 C.R. (6th) 213; *R. v. Mills*, [1999] 3 S.C.R. 668, 139 C.C.C. (3d) 321, 28 C.R. (5th) 207, 180 D.L.R. (4th) 1; *R. v. O'Connor*, [1995] S.C.J. No. 98, [1995] 4 S.C.R. 411, 103 C.C.C. (3d) 1; *R. v. Chaplin*, [1995] 1 S.C.R. 727, 96 C.C.C. (3d) 225; *R. v. Stinchcombe*, [1991] S.C.J. No. 83, [1991] 3 S.C.R. 326, 68 C.C.C. (3d) 1; *R. v. Bjelland*, [2009] S.C.J. No. 38, 2009 SCC 38. See also, Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111.

dent as to require that the "system integrity" concept of admissibility also dominate disclosure.

"Your Honour, I bring this application for disclosure and production of the 'source codes' of the many varieties of software that drive the electronic records management system from which the disclosure package comes, so that I might have that software tested for its integrity and reliability. For otherwise Your Honour, the Crown's case can hide behind its printouts without opportunity of cross-examination nor fear of accountability to 'full answer and defence'. The paper in the investigative file is but the end product of complex electronic technology applied to records management. A technology tested to give accurate results only to the point of being successfully marketable, and not to the point of being reliable beyond a reasonable doubt. Without 'disclosure and discovery' of the software and the system that produced those printouts, they have the dispositive power of an expert who can adduce expert opinion evidence, but does not have to testify, nor prove sufficient qualifications to give that opinion. That reverses the burden of proof and puts in place a *de facto* presumption of guilt, and also removes the opportunity to make full answer and defence."

(d) Records Management Networks are Vulnerable Like Blood Donation Networks

Paper record systems are physically separate such that they cannot infect or otherwise damage one another except by the transfer of paper records one to the other, and each such physical transfer cannot damage record systems around the world. But electronic records systems are intimately and continuously connected throughout the world such that they can all be infected and damaged disastrously in seconds. Electronic communications and the records they create are a "vital but vulnerable" foundation of our lives. They are as vulnerable as an international blood donations network. Viruses, worms, and other maliciously destructive software ("malware") launched on the Internet, create electronic communications technology's "blood infections." Therefore the reliability of the records they produce must be tested and protected with the same rigorous surveillance and regulation as that applied to donations of blood. And so must "proof beyond a reasonable doubt." And with this "vital but vulnerable network" concept of our use of electronic technology for RM, the "evidence to the contrary" presumptions and other reverse onus mechanisms of the electronic and business records provisions must be scrutinized. To reverse the onus of proof so as to place a burden upon the party who does not have access to, nor knowledge of the electronic records system whose "system integrity" is at issue, is to defeat the purpose of the electronic records provisions.

As lawyers and judges, we use sophisticated software and procedural security to protect and guarantee the reliability of our own electronic files from being attacked and corrupted by external and internal electronic operations and mischievous "malware" and spam, but then we go into court to apply admissibility rules of the weak "regular course of business activity" variety. They provide inadequate protection against the use of unreliable electronic records as evidence. The inconsistency is ignored — the inconsistency between the standards we apply to our own electronic RM systems, and that which we apply under the laws of evidence to impose substantial changes upon the lives of litigants, particularly so the involun-

tary litigants of the criminal courts. To say, "the *Evidence Act* rules," is not a sufficient answer when there are arguments above and below to make it rule differently. The case law, beginning with the amendment of the *Canada Evidence Act* in 2000, has produced no analysis yet of the electronic record provisions — no discussion of their underlying "systems" concept, or of what "system integrity" means and its proof requires. Therefore the disclosure and discovery case law won't either. They should go hand-in-hand. Both the admissibility and disclosure of records are now dependent upon the efficacy of the "system integrity" concept to create and make easy the "disclosure and discovery" of relevant records at the smallest time and cost.

(e) US Case Law

The American case law is now struggling with the same problems, but in relation to Federal Rule of Evidence 803(6) (FRE 803(6)), which is also being used in most states, or a provision similar to it, the FRE having been adopted as their state codes of evidence. It is a business record provision being used for electronic records. But like that in Canada, its case law provides no analysis yet of the conceptual and consequential factual and legal differences between traditional and electronic RM. Reading the American authorities in comparison, makes apparent how important is the choice of issue and the definition given to each of the three rules of admissibility for records: (1) the business record exception to the hearsay rule; (2) the best evidence rule; and, (3) the authentication rule. Categorization of an issue in some cases may have been guided more by the admissibility rule desired, and less by the integrity of the categorization.

II. ISSUE CATEGORIZATION DETERMINES THE APPLICABLE RULE OF ADMISSIBILITY

For example, in Canada, the authentication rule plays the minor role of requiring proof of authorship and authority to publish, or otherwise make known, a statement as that of the author. It is seldom invoked. In contrast, the following quotation from a law journal article written by experienced authors defines the use of the American authentication rule in terms that show it to be a test of the reliability of the evidence adduced; (the following is stated in reference to the use of computer animations and simulations):[8]

> As referenced by the *Insight Technology* court,[9] computer animations are most often used by practitioners as demonstrative evidence, "to illustrate and explain a witness's testimony," and to be admissible, must be "authenti-

8 Hon. Paul W. Grimm, (Chief United States Magistrate Judge for the United States District Court for the District of Maryland), Michael V. Ziccardi, (the 2008-09 law clerk to the Hon. Paul W. Grimm), Alexander W. Major, (a member of Venable LLP's Commercial Litigation group in Baltimore, Maryland, and part of the firm's E-Discovery Task Force), "Back to the Future: *Lorraine v. Markel American Insurance Co.* and New Findings on the Admissibility of Electronically Stored Information," (2009), 42 Akron L. Rev. 357, at 378.

9 *Insight Technology v. Surefire, LLC.*, Civ. No. 04-CV-74-JD, 2007 WL 3244092 at*2 (D.N.H. Nov. 1, 2007).

> cated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help to illustrate the testimony given in the case." Such a standard has been held to be applicable in both state and federal courts.

And if the hearsay exceptions are not demanding enough of the foundation evidence for admissibility, one's analysis can favour the use of the authentication rule. For example, for the distinction between computer-stored evidence and computer-generated evidence, the former can be left to some hearsay rule exception. But the more complex and risky computer-generated evidence should perhaps be submitted to the scrutiny of "authentication." Consider this passage from the same authors:[10]

> Despite the analysis in *Lorraine*,[11] the cases cited therein, and the authorities referenced in this Article, not all courts are so quick to draw the admittedly subtle distinction between computer-generated and computer-stored statements for purposes of determining whether the records produced by the computer are "statements" made by a "human declarant" for purposes of application of the hearsay rule. . . . The take-away lesson from *Lorraine's* discussion of Rule 801(b)[12] as it applies to electronic or digital evidence is that adherence to the five step analysis the opinion describes will ensure that the correct result is achieved — proper distinction between computer-stored statements initiated by a human declarant, which are excluded unless covered by a hearsay exception, and computer-generated non-hearsay statements, that are not admissible unless authenticated by showing that they were generated by a system or process capable of producing a reliable result.

It seems a dubious distinction given that humans provide everything that a computer is, has, and does. Therefore their renderings are as subject to human weaknesses as are humans themselves, whether producing computer-stored or computer-generated statements. Both should be subject to the same rule of admissibility (applied to suit each unique issue as to "truth of contents"), unless the time has come to employ a new rule. That appears to be where the American case law is now. This view is confirmed by the litigation and technology lawyer (attorney), George L. Paul:[13]

> However, in some cases, courts simply assume that computer-generated in-

---

10 *Supra* note 8 at 399-400.

11 *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007). As to the "five step analysis" this quotation refers to, the *Lorraine* decision states five questions for determining admissibility (at 538): (1) relevance, (2) authentication, (3) not a hearsay issue or is it admissible hearsay, (4) the "best evidence" rule, and (5) not unduly prejudicial. Using this "analysis" would not advance nor enhance the law in Canada.

12 (U.S.) Federal Rule of Evidence 801(b): "A 'declarant' is a person who makes a statement."

13 George L. Paul, *Foundations of Digital Evidence*, (American Bar Association, 2008), p. 119-20. The author is a partner and experienced trial lawyer in the Business Litigation Section of Lewis and Roca LLP in Phoenix, Arizona. His other books include, *The Authenticity Crises, The Discovery Revolution*, and, *Information Inflation: Can the Le-*

> formation is hearsay, without performing an analysis, seemingly avoiding the preliminary issue [of whether the information constitutes the "statement" of a "human declarant"]. These courts analyze objections to admissibility by searching for a hearsay exception, which they nearly always find. And courts that hold that computer-generated information is hearsay often complicate matters by using the term "computer-generated information" loosely, lumping all evidence that comes from a computer together, and failing to focus on whether what is really at issue is computer-*stored* information — often usually hearsay under anyone's definition. For example, in *United States v. Briscoe*, 896 F.2d 1476, 1493–95 (7th Cir. 1990) the court considered computerized "telephone records [that] listed the telephone numbers, the names of the subscribers placing calls to, as well as the subscribers receiving calls from, the three telephone numbers that were the subjects of [a] DEA wiretap investigation, the date, time and length of the call" to be hearsay, but did not parse which information, if any, was generated by a computer. The court simply assumed that the collective evidence was hearsay and analyzed the problem under the business records exception. [being (U.S.) Federal Rule of Evidence 803(6), reproduced in note 17 *infra*]
>
> This casual characterization of evidence coming from information systems renders the jurisprudence in the area somewhat murky. But, in many of the cases where courts actually analyze the hearsay issue, computer-generated evidence is rendered nonhearsay following the *Armistead* rationale,[14] reasoning that if you are not a human being, you cannot make a statement, and therefore hearsay cannot be involved, as there is no statement involved.
>
> . . . . .
>
> Now, *regularity* of preparation has become the key to admitting business records, including records containing computer-generated information. And if regularity is the test, almost any computer-generated information qualifies, without any showing of reliability. Accordingly, both the hearsay rule — and the main exception used to test admissibility of statements of information systems under it — become trivial, without any meaningful competency determination by the court. The ability to exclude out-of-court statements, the hearsay rule, appears to have largely evaporated with regard to computer-generated information. Rather, in almost every case, all computer evidence is admitted and things go to weight of the evidence. That may be our final, preferred policy, after rule makers and thinkers address this issue during the coming years, but in the meantime practitioners should acknowledge the reality of where the law has drifted.

After describing the weaknesses of computer systems, Paul concludes that no

---

gal System Adapt? He has been active in several sections of the ABA and of the Arizona State Bar concerning technology law and litigation.

14 *State v. Armstead*, 432 So. 2d 837 (La. 1983). The court held that a computer printout of telephone traces was "computer-generated data," and therefore not hearsay because the computer had recorded the source of the incoming calls independent of human activities. Therefore the court held the printout not to be a "statement" within the meaning of the hearsay rule, the assertions not having been made by a person.

distinctions should be drawn among such systems. "Statements of information systems are therefore hearsay."[15] Then, under the heading, "There Must Be a New Exception to the Hearsay Rule," he states:[16]

> But, notwithstanding their existence as hearsay, such statements will and must be admitted into evidence. There are too many such statements, and they are too important as evidence about our daily lives. Accordingly, there must be a properly considered exception to the hearsay rule. The business records exception is a creature of the mid-nineteenth century. But this problem is one of the late twentieth century and early twenty-first. It implicates not a compendium of human-entered statements, like the shop books of old, but the statements of information systems' reading and writing games. We need a new exception, or at least a consistent refinement to the closest one we have, Rule 803(6). As discussed, this exception should probably be called *systems reliability*.[17]

Accordingly, proponents of computer-generated information will need to lay a foundation to qualify statements as reliable under a systems reliability exception.

Paul is thus calling for a new interpretation of a business record provision,

---

15 *Supra* note 13 at 145.

16 *Ibid.*

17 (U.S.) Federal Rule of Evidence 803(6):

> Rule 803. Hearsay Exceptions: Availability of Declarant Immaterial
>
> The following are not excluded by the hearsay rule, even though the declarant is available as a witness:
>
> (6) Records of regularly conducted activity.
>
> A memorandum, report, record, or *data compilation*, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or *data compilation*, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, *unless* the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit. *[emphasis added]*

Accordingly, proponents of computer-generated information will need to lay a foundation to qualify statements as reliable under a systems reliability exception.

FRE 803(6), to incorporate a "systems reliability" test. Then it would better handle electronic records. Equally, that is the purpose of the, "system integrity" test.

In Canada, the "electronic records systems integrity test" of the electronic records provisions of the federal, provincial, and territorial Evidence Acts can perform that same function, which is what it was designed to do.[18] Therefore it must be considered the prime test of admissibility, not just a way of satisfying a rule that electronic technology has made useless — the best evidence rule. The latter should be restricted to traditional, non-electronic records. It was born of the errors of hand-copying from paper to paper; it should live to rule only there, separating the true "true copies" from the not-so-true.

Therefore, for more than 20 years American commentators have been calling for the abolition of the best evidence rule. For example, in 1992 the view that computer technology has made the best evidence rule irrelevant was put forward by Donald S. Skupsky, JD, C RM, an American lawyer, certified records manager, and expert on computer-produced business records. For several years prior he had argued for substantial changes to the best evidence rule, if its repeal could not be obtained. The following quotation from one of his articles is typical of other commentaries as to the incompatibility of the best evidence rule with electronic records as evidence:[19]

> THE NEW BEST EVIDENCE RULE
>
> The Best Evidence Rule needs immediate, radical changes. Any reference to the original records or paper records as the best evidence should be excluded from both legal philosophy and law. The Best Evidence Rule should be changed to indicate that accurate records, regardless of form, can be introduced in evidence or used for regulatory purposes.
>
> With the safeguards that can be built into today's modern records technology systems, the best evidence will not be the product of a particular technology but [the] result of a trustworthy process or system used to produce the records. Rule 901(b)(9) of the Uniform Rules of Evidence [and FRE 901(b)(9)][20] reflects what should be the criteria for introducing records into evidence. Under the title of "Identification and Authentication," ["Rule 901. Requirement of Authentication or Identification"] the rule establishes that

---

18 Only two of Canada's 14 jurisdictions, British Columbia and Newfoundland and Labrador, have yet to add electronic records provisions to the their "evidence" legislation. Quebec has comparable provisions in its *Civil Code of Quebec*, Book Seven, "Evidence," particularly: Articles 2831–2842, 2859–2862, and 2869–2874, and, *An Act to Establish a Legal Framework for Information Technology*, R.S.Q., c. C-1.1, ss. 2 and 68.

Given that all jurisdictions (except for the Northwest Territories) have enacted electronic commerce legislation, they will need express rules as to the admissibility of electronic records — commerce needs such rules to enforce its laws and practices. See Appendix B below, "A List of Electronic Commerce Acts and Electronic Record Provisions in the Evidence Acts in Canada."

19 Donald S. Skupsky, *The Best Evidence Rule is Dead . . . Except in the Mind of the Law*!, Records Management Quarterly, July 1992, 32–36, at 36, columns 2 and 3.

20 FRE 901(a), (b)(9) states:

> Rule 901. Requirement of Authentication or Identification

records (or other evidence) can be admitted in evidence if the proponent provides "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." This definition remains independent of a bias towards originals, duplicates, or any particular technology. The accuracy of the process or system used to produce the result will determine the legal acceptance of the records.

The Association for Information and Image Management [AIIM] has established a task force to prepare guidelines for the legal acceptance of records technologies based upon the accuracy of the process or system used to produce the results rather than the specific technology used. While the ultimate goal of this task force is to establish the guidelines for systems, the task force also seeks to eliminate laws that specify a preference for one technology or another. The findings of the task force clearly go contrary to the Best Evidence Rule.

CONCLUSION

The preference for original records makes no sense at this time in our history. Paper records are not inherently more reliable than other forms of records.

Paper records often result in the poorest, least accurate, and most unreliable form of records. Fraud can readily be perpetuated in paper records systems without a trace. Little or no sophistication is required to commit fraud since security for records is rarely provided.

Modern records technology systems, on the other hand, may utilize sophisticated equipment, establish procedures, audits, and other system components to ensure the integrity and accuracy of the system. While fraud is still possible, systems safeguards make it improbable while audit trails track the source of the problem.

Paper records are not best, but neither are records produced from modern records technology systems. Each form of record must be viewed based upon the accuracy of the process or system used to produce the record.

The time has come for the legal community to recognize that the Best Evidence Rule is irrelevant when it shows a preference for original paper records. The Best Evidence Rule is dead and has been dead for a long period of time. It is now time for the legal community to awaken to this reality.

(a) General provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

(b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

> (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

Unfortunately, the Uniform Law Conference of Canada chose otherwise for its *Uniform Electronic Evidence Act* (UEEA), a "model Act" that was used to draft the electronic record provisions. The "system integrity" admissibility test for electronic records in the UEEA is worded as "satisfying the best evidence rule," which is a contradiction. (See the list below of the eight points of contradiction under the heading, "5.(c) The Best Evidence Rule," p. 137.)

III. THE DIVERGENCE OF RECORDS MANAGEMENT PRACTICE FROM LEGAL THEORY UNDER THE BUSINESS RECORD PROVISIONS OF THE EVIDENCE ACTS

The theory of the law's reliance upon tests of admissibility and weight such as, "the usual and ordinary course of business," (s. 30(1) CEA (*Canada Evidence Act*); s. 35(2) OEA (Ontario *Evidence Act*); s. 23 NSEA (Nova Scotia *Evidence Act*))[21] and, "the circumstances of the making of the record," (s. 30(6) CEA; s. 35(4) OEA) is that it is always within a business's self-interest and conducive to the maximization of profit to maintain complete and accurate records. The need to maximize profit is presumed to be an unfailing and sufficient guarantee of complete and accurate records and RM systems, but in many situations now, incomplete and inaccurate records are necessary to minimize losses, which can be an incentive as powerful as the profit motive, because:

> (1) There are many more demands for production of records and information by private litigants and government departments and regulatory agencies than was the case when the theory, and the present law it supports, were created. Official agencies such as environmental, taxing, consumer, labour and securities authorities have much greater and more frequently used powers to force production of records, and disclosure of

---

21 This article cites throughout, the electronic records provisions of the Alberta, Nova Scotia, Ontario, and *Canada Evidence Acts* (using the designations: AEA, NSEA, OEA, and CEA). They are reproduced in the "Legislation Grid" in Appendix C below. It is not feasible to cite all of the Evidence Acts from all 14 provinces, territories, and the federal, *Canada Evidence Act*. The *Alberta Evidence Act* (like that of Newfoundland and Labrador) contains no business record provision. Therefore the business records exception to the hearsay rule at common law is relied upon. For the revised definition of that exception in Canadian law, see: *Ares v. Venner*, [1970] S.C.R. 608, 12 C.R.N.S. 349, 14 D.L.R. (3d) 4 (S.C.C.), and the case law it has generated. Hall J., delivering the judgment of the Court, defined the rule in the second last paragraph: "Hospital records, including nurses' notes, made contemporaneously by someone having a personal knowledge of the matters then being recorded and under a duty to make the entry or record should be received in evidence as prima facie proof of the facts stated therein."

See also the references to *Ares* and the common law exception in, Ken Chasse, "Electronic Records as Documentary Evidence" (2007), 6 Canadian Journal of Law and Technology 141, and in, J. Douglas Ewart, *Documentary Evidence In Canada* (Toronto: Carswell (now Thomson Carswell), 1984), and for business records in general, see the first three chapters, pp. 1–119. (Unfortunately Ewart's book is "out of print." In spite of its age, it contains the best treatment of the law concerning non-electronic records.)

information, and to conduct their own assessments, and searches and seizures under expanded legal powers. Such powers provide an incentive to "losing" damaging and embarrassing records and information in one's own records system. Often it is more conducive to profit and avoidance of loss to destroy or otherwise "lose" such records than to comply with demands for their production, even though such "spoliation" can bring severe penalties in legal proceedings, and in some jurisdictions it is a separate cause of action.[22]

(2) Often it is more important to corporate management to satisfy the investors and the fate of the stock they hold than it is to secure a profit in the marketplace. The income of senior management in public companies is usually focused on the stock price and stock options because stock price is often a basis for compensation and bonuses.

(3) The civil courts can be used to force production, disclosure, injunctions restraining competitive activities, and to obtain "Anton Pillar Orders," the civil search warrant. Therefore "damaging" records will not be left vulnerable to such processes.

(4) Many business, institutional, and government agencies have found that they can carry on business even though they have sub-standard electronic records systems, which indicates profit incentives are insufficient in themselves to produce high quality RM. (See the list of "common deficiencies" below in section 4.)

(5) Charitable and other non-profit organizations do not use a profit motive as an inducement to high quality RM.

(6) Many large commercial organizations, once feeling secure in their dominant position in the marketplace, take on a "social responsibility" mission as an additional strategy for preserving their dominance, rather than attempting to obtain optimum efficiency in pursuit of profit.

(7) Computer-to-computer transmission of data, both national and international, maximizes the weaknesses of electronic record systems because it greatly reduces human supervision of the transmission and manipulation of data, including the auditing of such systems for compliance with the recognized principles and practices. For example, "just in time" inventories, allowing manufacturers to maintain supplies only in sufficient quantities for daily or weekly production, require great amounts of documentation as to orders, acceptances, and deliveries, the necessary volume and speed of which dictate the use of computer-to-computer communications without human intervention.

(8) The use of several types of shared technology, such as "cloud com-

22 For a helpful analysis of the spoliation doctrine in Canada, along with a review of the caselaw to 1998, see, Craig Jones, "The Spoliation Doctrine and Expert Evidence in Civil Trials," (1998), 32 U.B.C.L.Rev. 293–325.

puting,"[23] reduces the security one can apply to one's electronic records system. The efficiency and lower cost achieved, also means less control of, and security for the system.

Such factors operate to undermine the ability of the profit motive and good business practice as sufficient justification for the "usual and ordinary course of business" test as being adequate for determining the admissibility of business records.[24] The business record provisions of the *Evidence Acts* are of dubious efficacy in limiting admissible records to "good" records. Therefore admissibility should require proof of good business practice in the management of records systems. But that is not what happens in court, neither in argument nor judgment. What should counsel advise the records manager as to what to expect as to admissibility, "weight," and electronic discovery? Today, it's better if the records manager advises counsel.

And the many corporate scandals of recent years of the Enron and WorldCom variety,[25] and the resulting legislation of the (US) *Sarbanes-Oxley Act 2002* kind,[26]

---

23 A definition of "cloud computing" can be found at: http://csrc.nist.gov/groups/SNS/cloud-computing; and, http://cloudsecurityalliance.org/

The Law Society of Upper Canada (Ontario) recently advertised to its members this audio seminar concerning the "cloud":

"Running a Virtual Law Office, November 15, 2010 12:00 p.m.–1:30 p.m.

"The virtual law office has moved from concept to reality. How can you connect an iPhone, Blackberry, and notebook computer to a "cloud" and stay on top of your files? What are the pitfalls of online backups and cloud storage? Learn about the possibilities and the responsibilities regarding confidentiality and its intersection with technology."

24 Applicable is the principle that, to justify the abandonment of a theory that is the foundation of an evidentiary provision determinative of admissibility, it is not necessary to show that it is no longer true in all, or even in most cases. It should be sufficient to show that there are competing inducements to inaccurate records management that make the current theory insufficient in itself to be determinative of admissibility.

25 See the Wikipedia entry: http://en.wikipedia.org/wiki/World_Com.

26 A significant reform of corporate governance, disclosure and accounting practices in the U.S. was the *Sarbanes-Oxley Act of 2002* ("SOX" or, Pub.L. 107-204, 116 Stat. 745, enacted July 30, 2002) also known as the, *Public Company Accounting Reform and Investor Protection Act of 2002*. It is a U.S. federal law enacted in response to a number of major corporate and accounting scandals including, Enron, Tyco International, Adelphia, Peregrine Systems, and WoldCom. These scandals cost investors billions of dollars when the share prices of the affected companies collapsed and shook confidence in the securities markets. SOX prescribes a comprehensive system of federal oversight relating to corporate governance and financial practices for companies that have issued securities in U.S. public markets and that file reports with the U.S. Securities and Exchange Commission (the "SEC"). It is a complex piece of legislation that was passed in response to the numerous, recent high-profile corporate and accounting scandals. The implications of SOX in the area of records management are considerable.

SOX is one of a number of recent Acts that have brought effective records management to the forefront of corporate concerns. CEOs and boards of directors now must imple-

(enacted in many countries, and it influenced certification requirements and audit committee standards in Canada[27]) indicate that the "profit motive" theory underly-

---

ment and constantly monitor records management programs to ensure their effectiveness. Given the many high-profile incidents of records mismanagement, one area receiving attention from lawmakers is how companies manage, retain and destroy their business records. SOX clearly holds companies and senior executives accountable, which underscores the need for comprehensive retention and destruction policies for documents and records generated by all participants in the corporate governance and auditing process. The consequences of non-compliance can be as severe as the demise of a company. For example, Arthur Andersen disappeared virtually overnight largely due to its disregard and abuse of records management policies and procedures. The U.S. Supreme Court exonerated the company on the question of criminal intent, but the company had ceased to exist by then.

SOX introduces important new recordkeeping provisions and mandates retention requirements for certain types of records. It also criminalizes and imposes severe penalties on executives and employees who obstruct justice by destroying or tampering with corporate accounting records. It creates a new federal crime for destruction, mutilation or alteration of corporate records with the intent to impede or influence a government investigation or other official proceeding or in relation to, or in contemplation of any such matter or case. This provision expands upon previous laws relating to the destruction of records with a presumed intent to obstruct justice. Previously, the law required a pending or imminent proceeding with a subpoena issued for the records that were destroyed. Under SOX, the government can bring charges of obstruction of justice if a company destroys potentially relevant records even *before* a subpoena is issued. In addition, it specifies minimum retention periods for auditor's work papers, correspondence, and other records that contain analyses, opinions, conclusions, financial data, or other information about corporate audits. SOX also creates an oversight board with broad authority to subpoena records produced by public accounting firms and their clients.

Prosecutions under SOX have been plentiful and the consequences severe. For example, in September 2004 Frank Quattrone, the most prominent investment banker of the 1990s "tech boom," was fined $90,000 and sentenced to 18 months prison and two years probation after being convicted of obstruction of justice. The charges brought against Quattrone appeared to be relatively minor. Prosecutors accused him of trying to block investigations when he forwarded an e-mail urging colleagues to "clean up their files."

27 In Canada, Bill 198, enacted by the Ontario legislature, protects investors by encouraging the accuracy and reliability of corporate disclosures. It came into effect on December 31, 2005 as Part XXIII.1 of the Ontario *Securities Act*. It created a statutory civil liability regime for misleading and inadequate disclosure by public issuers. For an analysis of Bill 198, see: Philip Anisman and Garry Watson, "Some Comparisons between Class Actions in Canada and the U.S.: Securities Class Actions, Certification, and Costs" (2006), 3 Canadian Class Action Review 467; see also: Philip Anisman, "Comments on Class Proceedings, Securities Market Liability and the CSA Proposal" in *Selected Topics in Corporate Litigation: Queen's Annual Business Law Symposium, 2000* 113 (Queen's University, Kingston Ontario, 2001).

Also, Canadian securities regulators adopted SOX-influenced certification requirements and audit committee standards and supervision in rules made under the securities laws. See the Ontario Securities Commission's website for National Instruments (rules)

ing the "usual and ordinary course of business" test is no longer a reliable guarantee of record accuracy and RM integrity.[28]

However, the "system integrity test" of the electronic records provisions (s. 34.1 OEA; ss. 41.1–41.8 AEA; s. 23D NSEA, and, ss. 31.1–31.8 CEA), can support an alternative application of the existing "admissibility" provisions.[29] No change need be made to their underlying "systems integrity" concept and test of admissibility (a record is no better than the system it comes from), but for consistency of terminology, the language of "best evidence" should be replaced with that of an "authentication" rule of the American variety.[30] It could be applied as an expanded "authentication" provision even though it labels itself as a "best evidence rule" provision. Given the frequency of software defects and failures, and an absence of a recognized and independent certification process for software and elec-

---

52-108 (auditor oversight), 52-109 (certification of financial statements and other disclosure obligations, and CP 52-109), and 52-110 (and CP52-110, on audit committees). Staff compliance review reports can also be found on the OSC's website. Therefore in Canada, as in the U.S., records management has now expanded from an important business process to a very important matter of "legal compliance."

28 Again, to justify the abandonment of a theory that is the foundation of an evidentiary provision determinative of admissibility, it is not necessary to show that it is no longer true in all, or even in most cases. It should be sufficient to show that there are competing inducements to inaccurate RM that make the current theory insufficient in itself to be determinative of admissibility.

29 The "system integrity test" is a shortform reference to these operative words in the electronic record provisions: "The integrity of the electronic record may be proved by evidence of the integrity of the electronic records system by or in which the data was recorded or stored, ..." (s. 23D(1) NSEA; s. 34.1(5.1) OEA; s. 41.4(2) AEA). Section 31.2(1) CEA has a very similar wording: "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, ..." Section 23D(1) NSEA: "In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or store." Section 23D(2) NSEA defines the "relied-upon printout"; see note 1, *supra*, and notes 35, 134 and 142 *infra*. And see the electronic record provisions in Appendix C, below, p. 178.

30 See for example, *In re Vee Vinhnee*, 336 B.R. 437, 2005 WL 3609376 (9th Cir. BAP Cal. 2005); and, George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008), Ch. 8, "The New Foundation of System Reliability," pp. 131–150. In *Vinhnee* ("filed" (released) Dec. 16, 2005), American Express credit card records were rejected for reasons that established a new and more detailed test of authenticity, and therefore better foundation evidence required for (U.S.) Federal Rule of Evidence ("FRE") 803(6) *supra* note 17, the business record provision under which the admissibility of electronic and non-electronic business records is determined. See the text accompanying notes 56–68 *infra*. It is concluded below that Canadian courts can similarly refurbish the business record provisions of the Evidence Acts in Canada to a badly needed increased efficacy.

tronic devices in general, such has practical and even necessary use.[31]

At present, the admissibility of electronic business records is determined by satisfying two sets of provisions. If a "hearsay" challenge is raised, the business record provisions are applied (s. 42 BCEA; s. 35 OEA; s. 23 NSEA; s. 30 CEA).[32] If in addition, a "best evidence rule" challenge is raised, the electronic record provisions are also applied. However, business records that have never been in electronic form (*e.g.*, paper records still in their "native" form, and those on traditional, pre-computer-driven microfilm) have to satisfy only the business record provisions. In the interests of trial efficiency, and simplifying preparation for trial, they should have been legislated into one provision.

In determining the admissibility of a business record that is an electronically recorded or stored record, one recent decision implies that the applicable business record provisions are to be satisfied first, and then the applicable electronic record provisions as well.[33] What is proposed here would require the reverse order, *i.e.*, the "authenticating" function of the electronic record provisions would be applied first, followed by an examination of the adduced record for compliance with the

---

31 Examples of recognized and authoritative certification processes are: (1) the Criminal Code's Alcohol Test Committee which certifies various makes and models of breathalyzer and intoxilyzer machines for use in relation to the impaired driving and "over 80" provisions (Can. Reg. SI/85-201 re s. 258 of the *Criminal Code*, R.S.C. 1985, c. C-46), and the "approved roadside screening devices" (Can. Reg. SI/85-200 re s. 254) and, (2) the Part 1, "Personal Information Protection" provisions of PIPEDA (the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5), s. 5 of which makes mandatory the application of the *Principles set out in the National Standard of Canada entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96* in Schedule 1 of the Act. And the following Quebec statute should be enacted as well in the other 13 jurisdictions of Canada, *An Act to Establish a Legal Framework for Information Technology* R.S.Q., 2001, c. C-1.1, in particular ss. 8 and 68 concerning the certifying of technology. This Act is Quebec's electronic commerce legislation, which serves the same purpose as *e.g.*, Ontario's *Electronic Commerce Act, 2000*, S.O. 2000, c. 17, and B.C.'s *Electronic Transactions Act*, S.B.C. 2001, c. 10. As to software failures in general and defects in relation to breathalyzer and intoxilyzer machines in particular, see: Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111, at 153–165.

32 "Hearsay" means a statement offered in evidence to prove the truth of the matter asserted within it, but made otherwise than in testimony at the proceeding in which it is offered: *R. v. O'Brien*, [1978] 1 S.C.R. 591 at 593-94; (1977), 35 C.C.C. (2d) 209 at 211 (S.C.C.).

33 See *R. v. Morgan* (January 10, 2002), [2002] N.J. No. 15 at ¶¶6, and 20 to 27, Flynn Prov. J. (N.L. Prov. Ct.). Morgan was charged with violating a fishing licence condition. A Crown witness tendered a computer generated copy of the fishing license and its conditions, and produced two affidavits attested to by the Acting Licensing Administration. Flynn, Prov'l. Ct. J., held that the electronic record provisions of the *Canada Evidence Act* cannot by themselves admit a document into evidence. Admissibility must be found by way of some other rule such as the business record provisions of s. 30 CEA. The electronic record provisions merely answer any objection based upon the best evidence rule. Note that subsections 31.2(1) and (2) CEA were accepted as being alternative means of answering such objections.

business record provisions. "Authentication" of an adduced record would require proof that it has been recorded or stored in or by an electronic record system having the required "systems integrity."

Also, electronic technology has blurred the distinction between "hearsay" issues and "best evidence rule" issues. It has made possible the separation of "data" from its "medium of storage" (*e.g.*, to read words and numbers, and to file and store them, they no longer have to be on a piece of paper or microfilm). Therefore in order to preserve (unnecessarily) the "best evidence rule," the electronic record provisions have had to redefine it as being the exact opposite of its traditional definition,[34] *i.e.* an "original" is now the last produced record and not the first produced record.[35] In regard to electronically-produced records, the "best evidence rule" should be repealed.

If, for example, a software failure casts doubt upon the truth of the contents of a printout, does that create a hearsay rule issue or a best evidence rule issue? "Truth of contents" issues are hearsay rule issues. But the electronic record provisions expressly treat electronic record systems and their printouts as creating best evidence rule issues — a printout is thus a "copy" of its electronic ("digital") source. Is the necessary answer that the hearsay rule applies to the declarations of human beings and not to those of electronic devices and the record systems that contain them? If it is not a hearsay rule issue, what is it? Perhaps therefore it is more correct to consider such as being the declarations of humans because it is humans who set such electronic systems in motion to make such declarations? The answer should be, "It doesn't matter how such issues are categorized!" The software failure has

---

34 The traditional best evidence rule states that where a fact or event is to be proved by means of a document or other recording, the "original" of such document or recording must be used unless an adequate explanation can be given for the absence of the original: *R. v. Cotroni*, 1979 CarswellOnt 78, 1979 CarswellOnt 48, [1979] S.C.J. No. 47, [1979] 2 S.C.R. 256, 45 C.C.C. (2d) 1 (S.C.C.); *Papalia v. R.*, [1979] S.C.J. No. 47, [1979] 2 S.C.R. 256, 45 C.C.C.(2d) 1.

35 The wording of the subsections that establish the "'system integrity' admissibility test" created by the electronic record provisions shows that the best evidence rule is recast to focus on the end product of the electronic information processing chain, rather than upon the first recording of information upon an "original" document. Electronic technology as applied to RM makes that necessary if one insists on perpetuating the best evidence rule from the paper into the electronic record world. Section 34.1(5) OEA states: "Subject to subsection (6), [the "relied upon printout" provision] where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic record." And s. 34.1(5.1) OEA states: "The integrity of the electronic record may be proved by evidence of the electronic record system by or in which the data was recorded or stored. . .." Section 31.1(1) CEA states: "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." Section 31.4 CEA provides for the making of regulations to establish evidentiary presumptions in relation to electronic documents signed with secure electronic signatures.

cast doubt upon the credibility of the contents of its printout.[36] The technology requires that the distinction between hearsay rule and best evidence rule issues be replaced by one concept, the reliability of electronic records. The required admissibility test will dictate the foundation evidence proving a sufficient guarantee of reliability. The electronic record provisions can provide that test. Then, the business record provisions must be removed or used to supplement that test.

IV. THE COMMON DEFECTS OF RM SYSTEMS AFFECT ADMISSIBILITY AND "WEIGHT"

The credibility of any part of a record system can be decisively damaged by defects in its other parts — "decisively," meaning the inadmissibility of any of its records when adduced as evidence. The "system integrity test" of the electronic record provisions (s. 34.1(5.1) OEA; s. 41.4(1), (2) AEA; s. 23D NSEA; s. 31.2(1)(a) CEA)[37] determines the admissibility of an electronic record by judging the "integrity" of the complete electronic records system, not just any particular part. However, those provisions also invite the use of recognized standards in aid of determining admissibility (s. 41.6 AEA, s. 23F NSEA, s. 34.1(8) OEA; s. 31.5 CEA).[38] Therefore the National Standards of Canada, *Electronic Records As Documentary Evidence* CAN/CGSB 72.34 ("*72.34*"), and *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB 72.11-93 ("*72.11*") must be ap-

36 The divergence between the theory and practice of the business record provisions is further analyzed in, Ken Chasse, "Electronic Records As Documentary Evidence," (2007), 6 Canadian Journal of Law and Technology 141 at 150-51 (issue 3, November, 2007); and, Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111.

37 This article contains several analytical references to the electronic records provisions of the *Alberta Evidence Act*, R.S.A. 2000, c. A-18, ss. 41.1–41.8 (AEA), the *Evidence Act* (Nova Scotia), R.S.N.S. 1989, c. 154 (NSEA), the *Evidence Act* (Ontario), R.S.O. 1990, c. E.23, 34.1 (OEA), and to the *Canada Evidence Act*, R.S.C. 1985, c. C-5, ss. 31.1–31.8 (CEA). See Appendix C below. Note that the OEA, AEA, and NSEA provisions use the terms, "electronic record" and "electronic records system"; the CEA uses, "electronic document" and "electronic documents system." Prior to "proclaiming in force" the CEA provisions in 2000, "document" meant a paper record (an electronic record printed out on paper). Now greater attention must be given to context because "record" and "document" will be used interchangeably because of this transgression in legislative drafting.

38 Without such reference to the relevance of standards, the use of the vague word "integrity," which is unprecedented in Canadian "admissibility" legislation, could make the electronic record provisions vulnerable to a "void for vagueness" attack. Standards, such as those cited above, provide sufficiently detailed principles and practices of RM so as to give the "system integrity test" a sufficient definition and ease of application that takes the electronic record provisions well beyond the realm of being "vague."

plied.[39] They have been developed by the Canadian General Standards Board.[40] They provide rules and procedures for RM with which to satisfy the tests and their undefined phrases in the Evidence Acts. They are based upon a "systems" concept of RM, as is RM itself.

There is no law specifically requiring compliance with these two standards as mandatory requirements of admissibility. But because they have been approved and promulgated by the Standards Council of Canada, and developed in accordance with the standards-development procedure required by the International Organization for Standardization in Geneva Switzerland (the ISO), they should be considered mandatory requirements. There is no competing standard or court decision. And, what is one's answer when accused of not being in compliance with such authoritatively recognized standards? Non-compliance will be taken as an absence of "system integrity."

A particularly important requirement of these standards is the "Prime Directive," which states (quoting *72.34*): "An organization shall always be ready to produce its records as evidence."[41] Failure to comply will risk a presumption of a lack of "system integrity."

As a truly objective test of undifferentiated application (unlike the very subjective "usual and ordinary course of business" test) the "system integrity" test should mean that a record system either has that essential "integrity" or it doesn't. A test is to be applied to the whole of a RM system, not just to parts of it. That interpretation of the test does not allow for admissibility obtained by proving the

---

39 See Appendix A, p. 174 "Summary of RM system compliance standards established by the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("*72.34*").

40 For example, in regard to *72.34*: "CAN/CGSB-72.34-2005" is its designation in Canada's National Standards System, which states that it is standard "72.34," (its shortform reference) developed by the Canadian General Standards Board (the CGSB), and approved in 2005 by the Standards Council of Canada, the coordinating body of the System. National Standards of Canada are written by standards-development agencies accredited by the Standards Council of Canada. Draft standards are submitted to the Council for its approval, and then published by the development agency. The Council's function is to ensure that the formal, established process for developing standards has been followed. On acceptance by the Council, they become National Standards of Canada. The national standards cited herein are those of the Canadian General Standards Board (CGSB), particularly, its newest electronic records standard, *Electronic Records as Documentary Evidence*-CAN/CGSB-72.34-2005, and its narrower predecessor, *Microfilm and Electronic Images as Documentary Evidence*-CAN/CGSB-72.11-93 (amended to April 2000). These standards are the work of committees composed of experts from the records and information management field, including legal advisors. They have been recognized by the ISO, the International Organization for Standardization in Geneva, Switzerland. The CGSB, a government agency within Public Works and Government Services Canada, has been accredited by the Standards Council of Canada as a national standards-development organization. The process by which such national standards are created and maintained in Canada is described within the Standard itself and on the CGSB's website (see, "Standards Development"), from which website these standards may be obtained, online: <www.ongc-cgsb.gc.ca.>.

41 Clause 5.4.3c at p. 17 of *72.34*, and subsection 4.1.2 at p. 21 of *72.11*.

"integrity" of only a particular part of a record system, even if the contents of a record adduced as evidence were directly affected by only a part. The test being a "system" test, there can be no valid argument that the sub-standard quality of other parts of the RM system not directly related to the production of the records in question are irrelevant.

No matter how good any one part of an electronic records system is from both a RM and legal point of view, in regard to legal proceedings its credibility and ability to satisfy the "system integrity test" is vulnerable to the defects in any other part of the RM system. Doubt cast upon a part casts doubt upon the whole. That will be the strategy for opposing the use of records as evidence — exploit a defect in any part of the RM system to defeat the records adduced from any other part of the system. Like the credibility of a witness as to sincerity, the "system integrity" of a RM system is a seamless whole. Therefore a legal opinion about a part of a RM system in relation to legal proceedings, must caution about the relevance of other parts of the system to issues concerning the admissibility and weight of records as evidence, and as to the requirements of electronic discovery. Therefore, the definition as to what is a "system" is critical to admissibility. Does an organization have one or many electronic records systems? Each separate "system" will have to comply with all of the requirements of the National Standards of Canada and not only the whole of an organization's records systems. Therefore it might facilitate the admissibility of records to operate the specialized RM functions by which they were recorded or stored as being part of one RM system. Deciding what is the scope, jurisdiction, and function of an RM system can be a complex question of fact without law that provides criteria for ascertaining whether an organization has one or many systems. And, given the complex world wide web of RM system connections and communications of data, case law is needed for determining whether a particular record is the product of one more RM systems.

For example, the "integrity" of a high quality imaging system will be harder to prove if opposing counsel can show that, in that same electronic records system: (1) email messages are not preserved and there is no email protocol regulating them as business records subject to RM system requirements; (2) there is no RM procedures manual as required by the National Standards of Canada; (3) the extent of records holdings is not known; (4) RM bylaws and orders from senior management are inadequate and (5) those that do exist are not complied with; (6) summaries and recordings of video, audio, and text communications are not made part of the RM system; and, (7) the "usual and ordinary course of business" in regard to RM is determined in a piecemeal, informal, and *ad hoc* fashion by various records officers as needs arise.

But, given the great capacity and flexibility of movement and manipulation provided by electronic RM, that has to be the rule and interpretation of "system integrity" — like human character and credibility, it is "of one piece" and not to be segmented into "good and bad" pieces, parts, and purposes.[42] Once possible to move and manipulate data (information) without a physical medium of storage such as paper and microfilm, anything can be done to and with it. That is why electronic

42 I use "electronic RM" in its widest sense to include optical and other digitized systems of manipulating and creating records.

records must be judged by the practice and reputation of the system they come from, and not simply by their own history, as is the case with the "usual and ordinary course of business" test of s. 30 CEA, 35 OEA, s. 42 BCEA, and s. 23 NSEA.

And apart from the needs of litigation, the same applies to the requirements of all legislation dependent upon high quality RM, *e.g.*, legislation concerning electronic commerce,[43] personal information protection and privacy,[44] electronic discovery,[45] and the records requirements of government departments and agencies.[46] A failure to satisfy the requirements of one will likely mean, and signal, a failure to satisfy all. Sharing a common "electronic RM foundation," they have a close interdependence and consequent failure.

The alternative interpretation of the "system integrity test," that it need be satisfied only in relation to those parts of an electronic records system that affected the record adduced as evidence and not all parts of the system is impractical. The concept is "systems integrity"; not, "part system integrity," and data can be too easily and inaccountably be moved throughout a system. And because one cannot know what future cases will demand of a record system, it is dangerous as well as impractical to leave the maintenance and updating of a system, or a part of it, until particular records are required. Alterations made "in contemplation of litigation" undermine the credibility of the entire system. They raise an inference that the system lacked the necessary "integrity" before such alterations. Also, such alterations and the records they produce would not be made "in the usual and ordinary course of business." Therefore such alterations would most likely result in a failure to satisfy both the electronic record and business record provisions of the Evidence Acts. That is one of the reasons why "the Prime Directive" of the National Standards of

---

43 For example, Ontario's *Electronic Commerce Act, 2000*, S.O. 2000, c. 17, and B.C.'s *Electronic Transactions Act*, S.B.C. 2001, c. 10.

44 For example, Part 1, "Personal Information Protection," of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5, which applies within provincial legislative jurisdiction as well as federal, until a province enacts its own *personal information protection Act* (a PIPA"), which displaces it in the provincial sphere. B.C., Alberta, and Quebec are the only provinces that have done so.

45 For example, Ontario *Rules of Civil Procedure*, Rule 29.1.03(4).

46 For example, the Canada Revenue Agency (CRA) informs the public of its polices and procedures by means, among others, of its *Information Circulars* (IC's), and *GST Memoranda*. In particular, see: *IC05-1*, dated June 2010, entitled, *Electronic Record Keeping*, paragraphs 24, 26 and 28. *Note* that use of the national standard cited in paragraph 26, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93 is mandatory for, "Imaging and microfilm (including microfiche) reproductions of books of original entry and source documents . . .." Paragraph 24 recommends the use of the newer national standard, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005, "To ensure the reliability, integrity and authenticity of electronic records." However, if this newer standard is given the same treatment by CRA as the older standard, it will soon be mandatory as well. And similar statements appear in the GST Memoranda, *Computerized Records* 500-1-2, *Books and Records* 500-1. IC05-1. *Electronic Record Keeping*, concludes with the note, "Most Canada Revenue Agency publications are available on the CRA web site www.cra.gc.ca under the heading 'Forms and Publications.'"

Canada cited herein[47] states, "an organization should always be prepared to produce its records as evidence." (Clause 5.4.3c of, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 (p. 17); and, paragraph 4.1.2 of, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93 p. 21). Compliance with "the Prime Directive" is a substantial part of compliance with the whole of the National Standards of Canada.

But what if all RM systems, as with some lawyers, are not thoroughly perfect practitioners; can they still claim to have the necessary "system integrity"? If, (1) the business record provisions can no longer provide adequate protection against the use of unreliable records as evidence, and, (2) there are many serious defects in RM practice that are very commonly found, then the "system integrity test" is badly needed, and needed to be the dominant test of admissibility if not the sole test thereof.

Serious defects in the management of electronic records systems are common even in the best of organizations. Each can taint the "system integrity" of the whole system. Among the most common, routinely found in the systems of large organizations, including those of government departments and agencies, universities, utilities, and commercial organizations are these:[48]

- the extent of the records holdings is not known;
- records are not properly classified nor indexed such that retrieval of records relevant to any particular subject is very difficult if not impossible;
- no definitive classification system among institutional, transitory, and personal records (e.g., which research and business records are those of each professor, and which are those of the university?);
- no records manual, or one that isn't kept current, or is not complied with;
- no bylaws (or orders of comparable authority from senior management) dealing with the records system — essential for establishing an organization's "usual and ordinary course of business" in regard to its records system;
- email is not classified, indexed nor pruned, or possibly not retained; there is no "email protocol" operative throughout the organization;
- records repositories are not well defined nor centrally accessible;
- no central policy for records management thus allowing the many divisions of the organization each to operate its own independent records system according to its own rules and practices;
- original paper records are not disposed of after being put into digital storage in a secure records management environment (with the exception of industry, professional, or special legal requirements as to retaining designated originals);

47 *Supra* note 40 and accompanying text.

48 This list of defects comes from the records management experts I work with on projects concerning the maintenance, alteration, and updating of large electronic records systems.

- image quality is not verified when original paper records are converted to electronic images, and there is no imaging manual dealing with the technical requirements for scanning paper records into electronic storage;
- metadata (data about data — data as to the management of records through time) is not used, therefore the biographical and bibliographical information about records is not used and properly maintained, therefore, *e.g.*, there are extensive duplicates and an inability to track official or original versions;
- no audit trails or controls detailing deletions, *i.e.*, when, who, by what retention-destruction/disposal authority?;
- no clear definition and practice as to what is the "deletion" of a record such that, *e.g.*, records may or may not continue to exist in backup storage thus diminishing knowledge of the extent of records holdings and their control;
- changes in technology result in unaccounted for and undocumented changes in records practice;
- no consistent practice as to other forms of communication that create records, *e.g.*, video and audio recordings, instant messaging, cellphone (mobile) communications;
- no "retention and disposal" program for records lifecycles;
- years after a merger or acquisition, the records system is still operating according to the conflicting rules of its component parts;
- no chief records officer with clearly defined and adequate authority;
- "orphaned data," *i.e.*, records that can no longer be retrieved or read because the new technology that now operates the records system is incompatible with the old technology that created those records (a "migration program" should accompany the installation of new technology);
- poor security protection;[49]

---

49 The ninth point of proof specified in the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 (*supra*, note 40 and accompanying text) section 5.5 states:

> i) security — security procedures are in place to protect the integrity of the records management system; at least the following should be able to be proved:
>
> 1. protection against unauthorized access to data and permanent records;
>
> 2. processing verification of data and information in records;
>
> 3. safeguarding of communications lines;
>
> 4. maintenance of backup copies of records to replace falsified, lost and destroyed permanent or temporary records;
>
> 5. retention and disposition of electronic records in compliance with legislated and internal retention periods and dis-

- inadequate compliance with the records management requirements of the privacy laws;[50]
- inadequate testing, auditing, and quality control;
- substantial non-compliance with the National Standards of Canada concerning records management, and a lack of appreciation of the consequences of non-compliance.

There is also an important "auditing consequence" for defective records systems. An auditor/accountant in testing the "internal controls" of a records system, may find that they cannot be relied upon.[51] Then the audit cannot be conducted using statistically based random sampling methodology to test the integrity of a series of records. A full substantive audit has to be done — which entails 100% verification. If cross examination of a records manager revealed that no reliance could be placed on the system and that a full substantive audit had to be done, that in itself would give significant support to an argument that the records from that records system should not be relied upon. The records system lacks "system integrity." Therefore the "system integrity test" of the electronic records provisions of the Evidence Acts has a strong similarity to auditing standards.

Such defects will result in (1) the "system integrity test" not being satisfied; (2) the demands of electronic discovery inadequately complied with; and, (3) admissibility refused, or, "weight" lost. For example, because of such defects, a disclosure request as simple as, "produce all records on subject X please," cannot be

---

position [disposal] requirements, and documenting such compliance and disposition schedules; and,

6. a business continuity plan for electronic records and associated data, including off-site copies of essential files, operating and application software [a "disaster recovery" factor].

50 For example, s. 5 in Part 1, "Protection of Personal Information in the Private Sector," of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, ("PIPEDA") makes mandatory, compliance with the National Standard of Canada, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, which is Schedule 1 of the Act. PIPEDA applies not only federally, but also in those provinces that don't have their own PIPA (*personal information protection Act*), which is all provinces except British Columbia, Alberta, and Quebec — see s. 26(2)(b) re exempting provinces. Part 2, "Electronic Documents," is the federal electronic commerce legislation (which has similar counterparts in 12 of the other 13 jurisdictions of Canada (NWT doesn't)), and Part 3, "Amendments to the *Canada Evidence Act*," added the electronic records provisions to the CEA, ss. 31.1–31.8 (which have similar counterparts in all of the other jurisdictions except for British Columbia and Newfoundland and Labrador).

51 For the principles, definition, and examples of, "internal controls," see these sites from the University of Florida website: http://fa.ufl.edu/uco/internal-control-checklist.asp

http://fa.ufl.edu/uco/internal-control-principles.asp

http://fa.ufl.edu/uco/guiding-principles-financial-management.asp

http://fa.ufl.edu/uco/internal-control-checklist.pdf

complied with, with complete certainty as to accuracy, comprehensiveness, and knowledge of the time, cost, and disruption to be incurred by answering such request. Therefore one cannot defend oneself against disclosure and discovery demands that violate the "proportionality test" that dominates the "discovery of documents" in the Rules of Civil Procedure and in the *Sedona Canada Principles*. One has to know one's RM system well, and have it operating well, to know what is disproportionate. But such defects will not be known if system documentation showing the state of the RM system is never requested nor examined. A RM system should be regularly "internally audited," and periodically independently, "externally audited."[52]

An electronic records system having the above defects cannot comply with the "prime directive" of the national standards: "An organization shall always be ready to produce its records as evidence."[53] In turn, it cannot comply with the "system integrity test" by which the admissibility of electronic records is to be determined.[54]

V. REVISED PURPOSES FOR THE ELECTRONIC AND BUSINESS RECORD PROVISIONS OF THE EVIDENCE ACTS

(a) Authentication

To determine how the tests of admissibility of electronic records might be changed, a comparison with the American rules is instructive. The American "au-

---

52 I have been the "legal advisor" on such external, independent audit teams with RM experts. That process provides a thorough system analysis and comprehensive certification of compliance with the two National Standards of Canada cited *supra* note 40 and accompanying text. But a quicker and less expensive procedure is needed for certifying such "systems compliance" for records to be used as evidence. Different reasons for such certifications should create different levels of certification. Therefore, the Canadian General Standards Board, the sponsor of these two standards, has been asked to consider establishing educational courses for RM specialists to become licensed, or otherwise official certifiers. See the discussion of this proposal in: Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111 at 163–65, and its recommendations 6 and 7 on p. 167.

53 *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005, clause 5.4.3 c) at p. 17; and, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93, paragraph 4.1.2 at p. 21, *supra* note 40 and accompanying text.

54 There are more than 200 specific compliance tests that the project teams I have worked with apply to determine the level of compliance of a records system with the national standard, *Electronic Records as Documentary Evidence*, *supra* note 40. There are more than 50 tests performed in relation to the earlier national standard, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93. The resulting report indicates the level of compliance found by each test, along with recommendations, and a legal opinion as to "legal compliance" with legislated records and RM requirements and consequences. See below section 11.(e), p. 169, "The transition from RM to 'legal compliance.'"

thentication rule" has a greater purpose than the Canadian rule[55] even though they use the same circular statement of the rule:

> Rule 901(a), (U.S.) Federal Rules of Evidence (FRE 901(a)): *General provision*. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that a matter in question is what its proponent claims.[56]
>
> Section 34.1(4) OEA: The person seeking to introduce an electronic record

---

55 The "minimalist" nature of the Canadian rule is confirmed by, John D. Gregory, "Authentication Rules and Electronic Records," (2002), 81 Can. Bar Rev. 529 at 562: "The trends of minimalism and technology neutrality dominate but do not hold the field exclusively." He describes (at 537) three factors of concern as to the reliability of electronic records under these three headings: "Uncertainty of storage; Uncertainty of retrieval; and, Ease of alteration, difficulty of detection." As to the nature of authentication he states (at 531): "Three questions arise in the process of authentication: What is this record? Where or who does it come from? Has its content been altered, either intentionally or unintentionally?" I suggest that differences as to the consequences of a ruling as to authenticity arise from the third factor, *e.g.*, to what degree is the record declared to be reliable? Is it merely an acceptance that the record appears to be what it purports to be, or is it in effect a preliminary decision as to reliability, *i.e.*, that the record is *prima facie* reliable?

56 Rules of Evidence for United States Courts and Magistrates, Pub.L. 93-595, S. 1, January 2, 1975, 88 Stat. 1926, as amended, Title 28 U.S.C.A. Most of the American states have adopted the Federal Rules of Evidence (the FRE) as their State codes of evidence, thus establishing the FRE as: (1) one of the most successful codifications of American law; and, (2) the foundation of the vast majority of state as well as federal case law concerning the U.S. law of evidence. It is therefore a small tragedy that Canada failed to enact the *Evidence Code* proposed by the Law Reform Commission of Canada's *Report On Evidence* (published in December 1975). The *Evidence Code* was a true code, and truly a close Canadian version (copy) of the FRE. Therefore the case law of the FRE would have been "free legal technology" flowing across the border to Canada had Parliament enacted the L.R.C.C.'s *Evidence Code* (as always, the provinces and territories would have copied it). For three years, 1976–78, I conducted the consultation process for the federal Department of Justice as to enacting the *Evidence Code*. That process and the resulting documentation produced by its "feedback" (resolutions) are described in, Ken Chasse, "Canada's *Evidence Code*?" (2006) 64 *The Advocate* 659 (published by the Vancouver Bar Association and distributed to all members of the Law Society of British Columbia). Because of the mixed reception the *Evidence Code* received (as described in the article), the resulting Federal/Provincial Task Force on Uniform Rules of Evidence proposed in 1981, a *Uniform Evidence Act*, which became (Senate) Bill S-31. But it too died. (However, the Task Forces's Report was published in 1982 by the Carswell Company.) Contradicting these comprehensive reform proposals, statutory reform of the law of evidence is now proceeding piecemeal, but very slowly. The addition of the electronic record provisions to the Evidence Acts, beginning in 2000, was the first significant reform of that variety. I was the Task Force's first "chair" and a member for the four years of its existence (1977–1981). For a definition and analysis of what is a "true code" (the *Criminal Code* is not), see: Ken Chasse, "The Meaning of Codification," (1976) 35 C.R.N.S. 178.

> has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be."[57]

These statements are not definitions of "authentication." They are merely statements as to the onus and burden of proof — who has to do the proving, what has to be proved, and with how much evidence (what degree of proof). George L. Paul, an experienced American litigation and technology attorney says this of the simplicity of FRE 901(a):[58]

> Clearly, no knowledge, either personal or institutional, about the immutability of the information in the record is required. No testimony is required about any processes that support immutability of information. What we have instead is a quick once-over with the information then coming into evidence and thereafter affecting the relevancy dynamics discussed previously. If you can introduce evidence of a routine, there is a presumption the routine was followed, even though it might not have been followed in that instance, or even if the "routine" is only a haphazard goal. There is no requirement about the quality of the routine, or how it would ensure immutability. These elements are assumed. The evidence is admitted, and the burden then shifts to the other party to disprove the information going to authenticity.

This description refers only to issues as to authentication. It does not mean that the record is admissible in spite of hearsay or best evidence rule challenges. However it does cast the American authentication rule as a rule by which *prima facie* admissibility in regard to authentication is established, *i.e.*, "a quick once-over," as to reliability. In contrast, the Canadian authentication rule serves only the more limited purpose of stating who has the burden of proving that a record is in fact what it purports to be. The American rule is considered to be an aspect of showing a record's relevance. After citing cases that indicate that the quantity and quality of the evidence necessary to authenticate depends on the ease with which the evidence can be altered or tampered with, Paul states[59]:

> There is therefore a tension in the authentication requirements under the Federal Rules. The language of Rule 901, and the greater weight of comment on the rules, view authentication foundations as issues of conditional relevancy and as governed by Rule 104(b). Under this view, so long as there is evidence whereby a rational jury could find an object authentic, there is a sufficient foundation to admit the evidence.
>
> FRE 104(b) states:
>
> *Relevancy conditioned on fact*. When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or

---

57 Section 41.3 AEA, s. 23C NSEA, and s. 31.1 CEA, are very similar to s. 34.1 OEA.

58 *Supra* note 13. George L. Paul, *Foundations of Digital Evidence*, (American Bar Association, 2008), p. 41. The author is a partner and experienced trial lawyer in the Business Litigation Section of Lewis and Roca LLP in Phoenix, Arizona. His other books include, *The Authenticity Crises, The Discovery Revolution*, and, *Information Inflation: Can the Legal System Adapt*? He has been active in several sections of the ABA and of the Arizona State Bar concerning technology law and litigation.

59 George L. Paul, *ibid.*, p. 44.

> subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.

The Canadian rule does not link authentication to relevance. Because it has this wider purpose, the American rule allows for greater scope for demands for electronic discovery of relevant documentation and information, which can also be used in relation to "weight."[60]

However, authentication of electronic business records would take on more effectiveness if guided by FRE 901(b)(9):

> *Process of system*. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

As stated by Cooper Offenbecher, an American commentator writing about the impact of *In re Vin Veehnee*:[61, 62]

> Indeed, such a presumption requires the opposing party to have detailed, affirmative knowledge about the computer systems. In these cases, however, the proponent is often the only party with access to the computer systems; the opposing party, conversely, usually lacks sufficient access to investigate potential sources of error. In today's fast-paced technological world, requiring the opponent to object to computer evidence likely puts an undue burden on the opposing party.[63] As a result, some argue that the Rule 803(6) foundation does not satisfy the basic authentication requirements of Rule 901(a), and that computer records always need to be authenticated under Rule 901(b)(9).[64] The method employed by *Vinhnee* incorporates many of these criticisms. It essentially puts the burden on the party offering the evidence to affirmatively demonstrate, through an eleven-step foundation process,

---

60 *Ibid.*, p. 49-50: "But remember that the main fight in any battle over truth is not the concept of admissibility, but rather the weight of evidence. If one wants to oppose a record introduced against your cause, you must be able to attack its probative force. Accordingly, there is a wealth of discovery and proof that can occur about the main facets of authenticity: about whether the information in a digital record has stayed the same through time; about the identity of who did what; and about the time at which certain events occurred. And similarly, if one wants to bolster a record, one shores up things through circumstantial evidence and *eunomic* regimes, if possible.

> "For example, . . . what do we know about the file before it was printed? Who had access to it? Does its custodian even know where it came from? Is there any trail or history of its evolution? Was it edited? When was it edited? By whom? Does the company that possesses the record have any information about these facts? And if it does not know about these facts, how can it know its records are authentic?"

61 *Supra* note 30 and accompanying text. The decision in *Veehnee* was released on Dec. 16, 2005.

62 Cooper Offenbecher, "Admitting Computer Record Evidence after In Re Vinhnee: A Stricter Standard for the Future?" (2007), 4 Shidler J. L. Com. & Tech. 6, at paras. 18, 20, and 23.

63 J. Shane Givens, "The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards," 34 Cumb. L. Rev. 95, 107 (2003-2004).

64 Mark A. Johnson, "Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability," 75 Marq. L. Rev. 439 at 464 (1992).

> that the offered record is in fact an accurate reflection of the information or record it purports to be.
>
> . . . . .
>
> The *Vinhnee* court seemed most concerned with the witness' knowledge of specifics regarding accuracy, security, and the potential for data error or loss. "There is no information regarding American Express' computer policy and system control procedures, including control of access to pertinent databases, control of access to pertinent programs, recording and logging of changes to the data, backup practices, and audit procedures utilized to assure the continuing integrity of the records."[65]
>
> . . . . .
>
> Regardless of what reasons the court actually had for excluding the records, it explicitly adopted the Imwinkelried "prism" as the court's means for evaluating the foundation.[66] In doing so, it rejected the sufficiency of the traditional Rule 803(6) foundation as self-authenticating and implicitly renewed the need to affirmatively authenticate computer records. The *Vinhnee* court's emphasis on reliability, accuracy, and system knowledge is consistent with urgings by the *Manual* [*The Manual for Complex Litigation*] and some scholars. Though it employs an eleven-step foundation process that has not previously been cited by courts, the key inquiries are into accuracy and reliability. These issues are not new and are the crux of traditional authentication inquiries in all areas of evidence. Imwinkelried's foundation process has been in circulation since 1980 and his *Evidentiary Foundations* book is a widely employed trial tool. In its essence, the Imwinkelried foundation is a well-articulated inquiry into accuracy and reliability. The *Vinhnee* approach is not, by nature, an outlier. It reflects a long-standing desire by some to inquire into the accuracy and reliability of computer records. While other courts may not immediately follow *Vinhnee*, the decision is unlikely to be eschewed as requiring unrealistic, exacting knowledge of records custodians.[67] The case may influence other judges who are similarly dissatisfied with the lack of knowledge of testifying witnesses.[68]

---

65 *Supra* note 13 at 448-449.

66 *Ibid.* at 447. Edward J. Imwinkelried is the author of a well-respected book on evidentiary foundations. Edward J. Imwinkelried, Evidentiary Foundations § 4.03[2] (5th ed. 2002).

67 *Vinhnee*, *supra* note 30, and Imwinkelried are cited positively and extensively in *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007), a memorandum decision denying summary judgment motions and detailing the law concerning the admissibility of computer records.

68 Most courts have held that Bankruptcy Appellate Panel (BAP) decisions are not binding on U.S. District Courts. See, e.g., *Bank of Maui v. Estate Analysis Inc.*, 904 F.2d 470, 472 (9th Cir. 1990). One court, however, has stated that BAP decisions are equivalent to the circuit courts and are therefore binding on all lower courts. *In re Globe Illumination Co.*, 149 B.R. 614, 620 (Bkrtcy. C.D. Cal. 1993), in the Ninth Circuit, for example, as a practical matter BAP decisions are regarded as persuasive by the Court of Appeals, and by district courts and bankruptcy courts within the circuit. *Appeals Before The Bankruptcy Appellate Panel Of The Ninth Circuit: A Manual For Litigants*, Summer 2007, available at

Clearly American commentators believe that the decision in *Vinhnee*[69] has established a new and more detailed inquiry into authenticity.[70] Cooper Offenbecher concludes:[71]

> However, the *Vinhnee* court marks an important step in the evolution of the comfort levels of courts with computer records. And while some litigators and witnesses may not be ready to produce the type of knowledge required to authenticate under the *Vinhnee* standard, they would be wise to take notice of this case as some courts are likely to begin requiring a more detailed foundation than Rule 803(6) requires on its face.

And Canadian courts can do the same for the authentication and business record provisions of our Evidence Acts.

Following Cooper Offenbecher's conclusion, the following "Practice Pointers" are stated:

> Businesses should have a designated "custodian of records" who knows the specifications of the hardware and software systems, processes for entering and extracting data from the computer, and the safeguards for accuracy and reliability.
>
> Witnesses who are called to authenticate computer records should be prepared to lay the *Vinhnee*/Imwinkelried foundation. There is generally no

---

http://207.41.19.15/Web/bap.nsf/cd1860ad415dbd4688256bc0006d5046/5e2253b1056e374288256ed2007766da/

69 *Supra* note 30 and accompanying text.

70 In addition to Cooper Offenbecher's article, *supra* note 62, the following are some of the available articles that analyze the decision in *Vinhnee*, *supra* note 30 (accessed on LexisNexis Quicklaw ("American journals") using the search term "Vinhnee").

> (1) Thomas R. McLean, MD, JD, FACS, "EMR Metadata Uses and E-Discovery" (2009), 18 Ann. Health L. 75.
>
> (2) Steven Goode, "The Admissibility of Electronic Evidence," 2009, The University of Texas School of Law Review of Litigation, 29 Recv. Litig. 1.
>
> (3) Keiko L. Sugisaka and David F. Herr, "SYMPOSIUM: The Twenty-Fifth Anniversary of the Minnesota Court of Appeals: EVIDENCE LAW: Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual?" (2009), 35 Wm. Mitchell L. Rev. 1453.
>
> (4) Hon. Paul W. Grimm, Michael V. Ziccardi, Esq., Alexander W. Major, Esq., "Back to the Future: Lorraine V. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information, (2009), 42 Akron L. Rev. 357.
>
> (5) Kathrine Minotti, "Evidence: The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession" (2009), 60 S.C. L. Rev. 1057.
>
> (6) Emily Burns, Michelle Greer Galloway, and Jeffrey Gross, "E-Discovery: One Year of the Amended Federal Rules of Civil Procedure, 64 N.Y.U. Ann. Surv. Am. L. 201.
>
> (7) David E. Ries, "Records Management: Current Issues in Retention, Destruction, and E-Discovery," (2007), 78 PA Bar Assn. Quarterly 139.

71 *Supra* note 62 at para. 24.

harm in laying too much foundation.

(b) The Exception to the Hearsay Rule for Business Records

In both Canadian and American business records exceptions to the rule against hearsay evidence, reliance is placed on the repetitive and routine nature of "a regularly conducted business activity" such as the making of business records. Section 35(2) OEA states:

> Any writing or record made of any act, transaction, occurrence or event is admissible as evidence of such act, transaction, occurrence or event if made in the usual and ordinary course of any business and if it was in the usual and ordinary course of such business to make such writing or record at the time of such act, transaction, occurrence or event or within a reasonable time thereafter.

And (U.S.) FRE 803(6) uses a similar phrase, "in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, ..." Note that both use a double "in the course of" phrase. But s. 30(1) CEA uses only a single phrase. US cases see an important distinction in the double phrase which distinction Canadian courts have not entertained, *viz.*, not only for example, must an accident report be made in the "usual and ordinary course of business," but also, having accidents must be part of the business.[72] Otherwise hearsay, such as accident reports, does not qualify for admissibility under the business records exception.

Most electronic business records are in fact the product of "regularly conducted business activities." Now, almost any such record can satisfy the business records exception without any showing of reliability or "system integrity." Almost all electronic records are admitted into evidence, which makes the only protection against using unreliable records as evidence, the assessment of "weight" (probative value; credibility) of records once admitted into evidence. But electronic RM is too complicated and vulnerable to error to allow its records to be given to the trier of fact without a preliminary investigation of reliability by way of an admissibility rule such as "system integrity." However there is a type of reliability (authentication) requirement in the wording of s. 30(6) CEA that allows, "the circumstances of

---

72 Compare the classic U.S. textbook cases of, *Palmer v. Hoffman*, 318 U.S. 109, 63 S.Ct. 477 (1943), *Johnson v. Lutz*, 253 N.Y. 124, 170 N.E. 517 (1930), which rejected such accident reports as not being part of the business's business, with the contrary result in, *Setak Computer Services Corp. v. Burroughs Business Machines Ltd.* (1977), 15 O.R. (2d) 750, 76 D.L.R. (2d) 641 (Ont. H.C.J.), wherein Griffiths J. stated (at p. 760 O.R.; p. 650 D.L.R.): "With respect, I believe that *Palmer* imposes an unreasonable and unnecessary limitation on the wording of the enactment [s. 35(2) OEA]. To draw a distinction between records relating to the principal business and those relating only to an auxiliary feature of the business, is not justified by the plain wording of the section. So long as the records are made in the usual and ordinary of some phase of the business, whether principal or auxiliary, they should be admitted, in my view, according to the plain meaning of s. 36 [now s. 35]." However, *Setak* did not involve a "record made in contemplation of litigation" as did *Palmer v. Hoffman*. Therefore in Canada, the double phrase has not imposed an additional requirement beyond what the single phrase in s. 30(1) CEA requires.

the making of the record" to be used to determine admissibility.[73] The FRE 803(6)'s comparable qualifying phrase is, "unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness." It too is a business record provision that will not provide adequate protection against unreliable electronic records being used as evidence if those words are not given an interpretation requiring proof of "electronic record system integrity." The case law shows no sign of it so far.

These traditional business records hearsay rule exceptions mistakenly attribute to electronic technology the fact that people become more accurate by carrying out the same activity repeatedly. Therefore the activity repeated within the "usual and ordinary course of business," and "the regularly conducted business activity," are assumed to be adequate guarantees of accuracy. But computer accuracy does not improve with repetition alone. Humans trained in "habits of precision" become more accurate. But computers, if programmed or operated incorrectly will always be wrong no matter the amount of repetition. Only a very small portion of software is self-correcting, because, *inter alia*, it requires built-in parameters as to what to look for and aspire to as being "correct."

What is needed is a "systems reliability" test that judges the quality of the whole electronic records system. Obviously the "system integrity test" could serve that purpose[74] as an authentication rule of the expanded type, to act as a first step to admissibility. The "systems integrity test" would be applied to ensure that the electronic records system from which the record comes complies with the recognized standards of RM, *i.e.*, the principles and practices established by the two National Standards of Canada cited above. Such issues are too complex to be left to "weights" and to juries.

Then a second test would be applied to the record itself to verify that there is no "circumstance of its making" requiring its exclusion. This need can be served by provisions such as s. 30(6) CEA, which is an exclusionary rule that determines if the admissibility rule in s. 30(1) CEA applies, *i.e.*, is there some "circumstance of the making of the record" that justifies excluding it even though "made in the usual and ordinary course of business"?[75]

---

73 Section 35(4) OEA and s. 23(4) NSEA contain similar words, but such examination of "the circumstances of the making" are restricted to use in relation to "weight" and prohibited from being used in relation to admissibility. The better opinion of s. 30(6) CEA is that it, and not the "usual and ordinary course of business" test in s. 30(1) is dominant test because any such "circumstance" could be used to rule any record inadmissible. However, s. 30(6) is an exclusionary rule and not an inclusionary rule as is s. 30(1). The other view is that s. 30(6) is applicable only to weight; see: Ken Chasse, *Electronic Records As Documentary Evidence* (2007) 6 Canadian Journal of Law and Technology 141, at section, "4(b) The Two Hearsay-Admissibility Tests of s. 30 CEA — Which is Predominant?"; and, J. Douglas Ewart, *Documentary Evidence In Canada* (Toronto: Carswell, 1984) at p. 85, footnote 57 of that text.

74 To best serve that purpose, the references to the "best evidence rule" should be removed to prevent any interpretation that reduces the importance of that purpose.

75 Section 35(4) OEA, and s. 23(4) NSEA restrict the use of such "circumstances" to "weight." It would have to be amended to serve the same purpose. But s. 35(2) OEA and s. 23(2) NSEA do have a double "course of business" test, whereas s. 30(1) CEA

These interpretations would accomplish these purposes: (1) ensure that all of the unique features of electronic RM systems, as distinguished from those applicable to pre-electronic paper systems, are judged as in compliance with recognized standards; and, (2) the existing legislation is used with a minimum of revision needed and none not absolutely necessary. They will help to move admissibility issues beyond an unquestioning faith in the evidence produced by science and its electronic devices, but within a manageable time allowance in court or tribunal proceedings to accommodate them.

(c) The Best Evidence Rule

The above purposes for the business record and electronic record provisions of the Evidence Acts leave no room or need for the best evidence rule. References to it in the Evidence Acts should be removed, and until then, one's arguments as to admissibility made stronger by denigrating it — "system integrity" is not a mere matter of "best evidence." Electronic technology, as applied to RM, has no place for it, therefore neither should the laws of evidence that determine when and how electronic records are to be used. The best evidence rule was developed at a time when making a copy required copying by hand to make a copy. It was not possible to have a record without its also being recorded on a medium of storage such as paper. Therefore issues as to copies were easily distinguished from issues as to "the truth of the contents" of a document. For the former, the best evidence rule was applied; for the latter, the hearsay rule and its exceptions were applied. The two rules provided different solutions for very different problems.

But now there is data without a physical, viewable medium of storage, which is nonetheless a record — a record in electronic form, which can be viewed and altered apart from any particular medium of storage. And so there are records that are "original records" but they have no medium of storage in the traditional sense. And it is frequently not possible to distinguish which activities of computers concern "the truth of the contents of a record" (a hearsay issue), and which concern the authenticity of a record, and which concern the laying down of a record upon a medium of storage and accessing and printing it from that medium — any and all storage, be it magnetic, optical, mechanical, chemical, genetic, paper, or stone tablet (a best evidence rule issue). As a result, distinguishing which one of these three rules applies is more than just somewhat arbitrary. For example, a software failure that casts doubt upon the truth of the contents of a printout, does not require categorization as giving rise to a hearsay rule issue or a best evidence rule issue. If there is doubt as to the credibility of the printout, that is the legal issue to be dealt with, and it requires no further categorization or naming before legal analysis based upon "system integrity" can begin.

Drafting the electronic record provisions as a variety of the best evidence rule

---

has only the single phrase. So far, the case law has not made a distinction as to the legal consequences of the difference; see: *Setak Computer Services Corp. v. Burroughs Business Machines Ltd.* (1977), 15 O.R. (2d) 750, 76 D.L.R. (2d) 641 (Ont. H.C.J.). The double phrase could be interpreted as providing the same exclusionary mechanism that is provided by s. 30(6) CEA.

makes them a contradiction of the traditional rule:

> 1. It stands the rule on its head by making the last produced record and printout the "original," instead of the first made recording of the contents of the record, as does the traditional best evidence rule.
>
> 2. The electronic record provisions state, "where the best evidence rule is applicable . . .." Where and when is that? Given this very unconventional and unprecedented usage, how does one know how to frame, or answer an objection based upon the best evidence rule? Falling back on the traditional rule as the only resource, one looks for an "original" and a "copy," but with no guidance as to how those concepts apply to electronic records. Then perhaps one should use the "*McMullen* standard"?[76] But that formula requires proof of the equivalent of the "system integrity test," which is where one starts when attempting to use the electronic record provisions.
>
> 3. How to see or compare the electronic "original" of a printout other than by the printout itself or a screen display of that "original," *i.e.*, the copy cannot be compared with its "original" to determine if it is a "true copy."
>
> 4. The traditional best evidence rule concerns, "copies, duplicates, and other secondary evidence of an original record," but not the "system integrity" of a whole records system, in all aspects of records management "integrity"!
>
> 5. The former is a "records" concept, the latter is a "systems" concept; this is using terminology merely for the sake of using traditional terminology.
>
> 6. The traditional rule determines the form in which a record is to be adduced; the "system integrity test" determines the "integrity" of the record adduced, and that "integrity" bears heavily upon "the truth of the contents" of that record, if not completely determining its outcome.
>
> 7. Therefore the "systems integrity test" well serves the purpose of a records exception to the hearsay rule, (or an American "authentication" rule) which is not the purpose of the traditional best evidence rule.
>
> 8. In regard to electronic records, the best evidence rule (as used in the electronic record provisions in Evidence Acts in Canada) is to safeguard against the use of unreliable records as evidence, but in regard to non-electronic paper records, it will protect only against inadequate copies and duplicates of those records.

These points do not detract from the important improvements brought to the law by the "system integrity test," but it shouldn't have used the terminology and concept of the best evidence rule. In fact, the following improvements brought to the law by the electronic records provisions of the Evidence Acts show how inap-

---

76 For the passage of *McMullen* (OCA, 1979) stating the "*McMullen* standard," for the admissibility of electronic records, see notes 122 to 125 *infra* and accompanying text.

propriate a foundation concept the best evidence rule provides for them:

> 1. Substitute an evaluation of "electronic record system integrity" in place of evaluating paper-original documents as a test for determining the admissibility of, and "weight" (probative value; credibility) to be given business records (ss. 31.2 & 31.3 CEA; s. 34.1(5)–(7) OEA; ss. 41.4 & 41.5 AEA; ss. 23D & 23E NSEA), particularly so if they were to subsume the business record provisions, because satisfying the "system integrity test" will satisfy the subjective "usual and ordinary course of business" test of the business record provisions;
>
> 2. Expressly encourage the use of: (1) national, international, and industry standards of records and information management in the determination of issues of admissibility and weight of electronic records; and, (2) recognize private evidentiary agreements and protocols for computer-to-computer communications, *i.e.*, EDI (electronic data interchange) for transmitting all business records electronically, and for settling disputes arising from such data interchange (s. 31.5 CEA; s. 34.1(8) OEA; s. 41.6 AEA; s. 23F NSEA)[77];
>
> 3. Abolish retention periods for paper-original records as a condition-precedent to the admissibility of their microfilm and imaged counterparts (the infamous "six-year rule"; *e.g.*, s. 34(3), (4) OEA repealed — but such repeal not being necessary for s. 31 CEA because it did not contain a retention period);
>
> 4. Give electronic records a legal status equal to that of paper-originals in regard to the authentication rule and the best evidence rule (ss. 31.1 & 31.2 CEA; s. 34.1(4), (5), (5.1) OEA; ss. 41.3 & 41.4 AEA; ss. 23C & 23D NSEA);
>
> 5. Make destruction of paper-originals optional without impairing the legal status of their electronic record counterparts in relation to admissibility and weight.[78]

---

77 These two functions are captured in the words, ". . . evidence may be presented in any legal proceeding in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, ..." For example, two companies could have a private agreement setting rules as to their computer-to-computer communications concerning orders, invoices, and deliveries. Note that such "standards, etc.," can be used "For the purpose of determining under any rule of law whether an electronic record is admissible, . . . "*i.e.*, not just for determining admissibility under the electronic record provisions alone.

78 Destruction of original paper records after scanning or otherwise imaging them into a secure electronic records management environment (national standard *72.34*, Section 5 "Legal Requirement," Section 5.1 "General"; see notes 40 and 52 *supra*, and accompanying text), can be assumed to be optional because the electronic records provisions of the Evidence Acts are silent as to such disposal and destruction after making such electronic versions or counterparts. But records management retention-destruction/disposal programs are always subject to the "litigation hold" required to be placed upon such programs (suspending their operations) by demands made in electronic discovery proceedings. Such obligations arise "on contemplation of litigation," and not only when

None needs nor makes appropriate the use of the best evidence rule. Then why was it used? The electronic record provisions were created to render irrelevant doubts as to the ability of the business record provisions to cope with electronic records, but to do so without disturbing those provisions and their treatment of the business record exception to the hearsay rule. Therefore, the electronic record provisions could not be a hearsay rule or exception thereto. The doubts were not evident in the case law as to s. 30 CEA and its provincial counterparts, but rather in the other forms of analytical legal literature. In fact, the case law on s. 30-type provisions did not show it (or them) to be "broken" at all, therefore, "why fix it?" Section 30 CEA wasn't "broken," rather, it wasn't "built right" in the first place.[79]

---

litigation commences or is ongoing. Otherwise, paper originals should be disposed of once moved to secure electronic storage. As long as the paper is accessible, production of it can be demanded for comparison with its electronic version.

79 The then Minister of Justice and Attorney General of Canada, John Turner, told the House of Commons on January 20, 1969, (Hansard, House of Commons Debates, p. 4496) on Second Reading of the present s. 30 CEA: "It is therefore apparent that the law in this country has fallen far behind the major changes which the computer age has brought to business methods." And he justified s. 30's low "threshold of admissibility" as follows: "I consider that, in general, the law of evidence should be moving away from the rigid rules of admissibility toward assessment of the cogency of logically relevant facts. If the facts are relevant, what is the best way to introduce those facts without there being any unfairness to either side? Accordingly, Mr. Speaker, this bill would, subject to certain safeguards, render business records as defined in the bill generally admissible and would entrust the courts with the discretion of assessing the probative value of those documents." In fact to the contrary, the "computer age" has necessitated a more demanding and objective standard for admissibility as exemplified by the electronic record provisions such as ss. 31.1 to 31.8 CEA.

I have read the Department of Justice files generated by the creation of s. 30. They show (1) a dominant intention to cope with the decision in *Myers v. D.P.P*, [1965] A.C. 1001; (2) an absence of any concern that electronic technology would require a change in the admissibility rule as to business records (*Myers* did not involve electronic records); (3) a bias towards admissibility because most issues were believed best left to "weight"; and, (4) the belief that the reliability of business records is sufficiently assured by proving that they are the product of a regularly conducted business activity. Therefore, with the guidance, approval, and correspondence of Sir Rupert Cross, the author of the leading British, Evidence textbook at that time, the phrase, "the usual ordinary course of business" became the key phrase in the business record provisions of the Evidence Acts in Canada. It was taken from American law reform proposals such as s. 63(13) of the Uniform Rules of Evidence drafted by the National Conference of Commissioners on Uniform State Laws in 1953. And today, Rule 803(6) of the (U.S.) Federal Rules of Evidence (the "FRE") uses the phrase, "in the course of a regularly conducted business activity," to determine the admissibility of a "data compilation, in any form." Thus an "electronic records admissibility test" for "business records" is provided by a single subsection within a section of several hearsay exceptions — the kind of order that codification can provide. But like the Canadian business record exceptions, Rule 803(6) depends upon proof of a repeated "course of business" business activity as the guarantee of record reliability. However, it isn't unnecessarily

VI. THE DEFICIENCIES OF THE BUSINESS RECORD PROVISIONS OF THE EVIDENCE ACTS

Section 30 CEA, and the business record provisions of the provincial and territorial Evidence Acts, still have the several major deficiencies with which they were enacted, which are still in need of case law or legislative solutions. Further compounding these difficulties is the absence of definitions of key phrases — a legislative drafting style intending flexibility, rather than doubt as to intended meaning, usage, and scope.

The current law as to the admissibility and weight of business records is based upon three concepts, two of which are without fixed definitions and the third needs to be revised for electronic records. The two undefined concepts are, "the usual and ordinary course of business;" and, "the circumstances of the making of the record." They appear in most of the Evidence Acts in Canada.[80] The third is the concept of the "original" record.[81] The absence of fixed definitions of these key phrases gives the courts complete flexibility in applying them. But that same flexibility leaves litigants and the business community uncertain as to what is required to prove business records as admissible, credible, and persuasive evidence. And, several important hearsay rule questions about business records as evidence remain unanswered, even with the combined assistance of statutory business record provisions and court decisions interpreting them.

Consider the following examples of important questions needing answers, or new answers, and the conflicting answers given by the court decisions cited in their accompanying notes:

> Whether the present statutory language requires that admissible records need only be made by a person under a "business duty" to make such records, or whether the supplier of the information recorded, as well as the maker of the record must have been acting pursuant to such "business du-

---

spread out over two sets of subsections as are the electronic and business records provisions of the Evidence Acts in Canada.

80 See for example s. 30(1), (6) CEA, s. 35(2), (4) OEA, s. 23(2), (4) NSEA. While these OEA and NSEA provisions contain a double "usual and ordinary course of business" test (as do most of the provincial Evidence Acts), the CEA provisions contain a single test, and whereas the CEA makes the "circumstances of the making of the record" relevant to both admissibility and weight, the OEA and NSEA counterparts in s. 35(4) OEA and s. 23(4) NSEA expressly restricts the relevance of such "circumstances" by the words, "may be shown to affect its weight, but such circumstances do not affect its admissibility."

81 Before computers were used to create and store business records, the words "record" and "document" could be used interchangeably because all records were in the form of paper documents. But separating the concepts of the content of a record from the medium upon which it was stored made necessary the use of a different word for each, that is, "record" for the content of the record, and "document" for the medium upon which it was stored or written. Similarly, "data" makes a "record," which when stored on paper, becomes a "document." But now the CEA uses "document" in its electronic record provisions, while most of the other Evidence Acts use "record," and, the CEA itself uses "record" in its business, banking, and microfilm record provisions (ss. 30, 29, and 31). Therefore the inconsistency in the CEA is inexplicable.

ties".[82] For example, a customer using an ATM is not under a business duty to the bank but bank records are thus made by that customer and relied upon by the bank.

Whether s.30(1) CEA allows for double hearsay (twice removed from the person having direct personal knowledge) and not just single hearsay (once removed). Such limitation would arise from the opening words, "Where oral evidence in respect of a matter would be admissible . . .."[83]

Whether it is sufficient if the making of the record was part of the ordinary course of the business, or whether not only the making of the record but also the events being recorded must be part of the business routine.[84] For example, making an accident report is business routine, but the accident is not,

---

82 See for example the following decisions: *R. v. Felderhof*, 2005 ONCJ 406, 201 C.C.C. (3d) 384, 2005 CarswellOnt 4726, [2005] O.J. No. 4151 (Ont. C.J.) [*Felderhof*]; *Setak Computer Services Corp Ltd. v. Burroughs Business Machines Ltd et al.* (1977), 15 O.R.(2d) 750, 76 D.L.R.(3d) 641 (Ont. H.C.); *Waltson Properties Ltd., Re* (1976), 17 O.R. (2d) 328 (Ont. H.C.); *Matheson v. Barnes* (1980), [1981] 2 W.W.R. 435 (B.C. S.C.); *Adderley v. Bremner* (1967), [1968] 1 O.R. 621 (Ont. H.C.) [*Adderley*]; *Canada (Ministre de la Citoyenneté & de l'Immigration) c. Obodzinsky*, 2003 CarswellNat 1351, 2003 CarswellNat 551, [2003] A.C.F. No. 370 (Fed. T.D.); *R. v. Monkhouse*, 1987 CarswellAlta 248, [1987] A.J. No. 1031 (Alta. C.A.); *Catholic Children's Aid Society of Toronto v. L. (J.)*, 2003 CarswellOnt 1685, [2003] O.J. No. 1722, 39 R.F.L. (5th) 54 (Ont. C.J.) [*Catholic Children's*].

83 *R. v. Gregoire*, 1998 CarswellMan 451, [1998] M.J. No. 447, 130 C.C.C. (3d) 65 (Man. C.A.); *R. v. Grimba* (1977), 38 C.C.C. (2d) 469 (Ont. Co. Ct.); *R. v. Martin* (1977), 8 C.R. (5th) 246 (Sask. C.A.); *R. v. Wilcox*, 2001 CarswellNS 83, [2001] N.S.J. No. 85, 152 C.C.C. (3d) 157, 192 N.S.R. (2d) 159 (N.S. C.A.), [*Wilcox*]; *Canada (Minister of Citizenship & Immigration) v. Oberlander* (1998), [1999] 1 F.C. 88, 153 F.T.R. 11 (Fed. T.D.); *Canada (Minister of Citizenship & Immigration) v. Skomatchuk*, 2006 FC 730, 2006 CarswellNat 1634, 2006 CarswellNat 4746, [2006] F.C.J. No. 928 (F.C.); *R. v. Sunila (No. 2)* (1986), 26 C.C.C. (3d) 331 (N.S. T.D.) [*Sunila*]; *R. v. Marini*, 2006 CarswellOnt 6215, [2006] O.J. No. 4057 (Ont. S.C.J.); *Baker v. R.* (1977), 35 C.C.C. (2d) 314 (B.C. C.A.); *R. v. Scheel* (1978), 42 C.C.C. (2d) 31 (Ont. C.A.).

84 *Setak Computer Services Corp Ltd. v. Burroughs Business Machines Ltd et al.* (1977), 15 O.R.(2d) 750, 76D.L.R.(3d) 641 (Ont. H.C.); *Aynsley v. Toronto General Hospital* (1967), [1968] 1 O.R. 425 (Ont. H.C.); varied 1969 CarswellOnt 888 (Ont. C.A.); affirmed 1971 CarswellOnt 170, 1971 CarswellOnt 170F (S.C.C.); *Palter Cap Co. v. Great West Life Assurance Co.* (1935), [1936] O.R. 341, [1936] 2 D.L.R. 304 (Ont. H.C.); reversed 1936 CarswellOnt 156 (Ont. C.A.); *Conley v. Conley*, [1968] 2 O.R. 677, 70 D.L.R. (2d) 352 (Ont. C.A.); *British Columbia v. Harris*, 2003 BCSC 1257, 2003 CarswellBC 1981, [2003] B.C.J. No. 1897 (B.C. S.C.); *Newmarket (Town) v. Halton Recycling Ltd.*, 2006 CarswellOnt 3371, [2006] O.J. No. 2233 (Ont. S.C.J.); additional reasons at 2006 CarswellOnt 5284 (Ont. S.C.J.); *Robb Estate v. St. Joseph's Health Care Centre*, 1999 CarswellOnt 500, [1999] O.J. No. 523 (Ont. Gen. Div.) [*Robb*]; *Catholic Chilren's Aid Society of Toronto v. J.L.* (2003), 39 R.F.L. (5th) 54, [2003] O.J. 1722 (Ont. S.C.); *Johnson v. Lutz et al.* (1930), 253 N.Y. 124, 170 N.E. 517 (C.A. of New York); *Palmer v. Hoffman* (1943), 318 U.S. 109, 63 S.Ct. 477 (USSC).

unless one's business is accidents.

Whether contemporaneity (co-incidence in time) between the making of a record and the events recorded as part of the "usual and ordinary course of business" must always be required, or at least considered.[85]

Whether records are inadmissible because of the interest or bias of the maker of the records, or whether such a requirement is not to be read into the business record provisions of our Evidence Acts, and is merely to be considered as to the "weight" of the record if admitted into evidence.[86]

Whether admissibility requires detailed evidence of the RM system, or merely an examination of the system by an expert witness of the proponent of the records in question.[87]

Whether business records may contain statements of opinion.[88]

And the Supreme Court of Canada has held that a computer printout can be treated as an "original" business record even if its electronic source has been deleted. Previously, the hardcopy printout was held to be merely a copy dependent upon the continued existence of its electronic counterpart for pur-

---

85 *R. v. Felderhof* (2005), 201 C.C.C. (3d) 384, [2005] O.J. No. 4151 (Ont. S.C.); *Setak Computer Services Corp Ltd. v. Burroughs Business Machines Ltd et al.* (1977), 15 O.R.(2d) 750, 76D.L.R.(3d) 641 (Ont. H.C.); *R. v. Vanlerberghe* (1976), 6 C.R. (3d) 222 (B.C. C.A.) [*Vanlerberghe*]; *R. v. West*, 2001 CarswellOnt 2960, [2001] O.J. No. 3413 (Ont. S.C.J.) [*West*]; *Robb v. St. Joseph's Health Care Centre*, [1999] O.J. 523 (Ont. Ct. G.D.); *Re S.V.*, [2002] S.J. No. 714 (Sask. Q.B.).

86 *Northern Wood Preservers Ltd. v. Hall Corp. (Shipping) 1969 Ltd.*, [1972] 3 O.R. 751 (Ont. H.C.); affirmed (1973), 2 O.R. (2d) 335 (Ont. C.A.); *Setak Computer Services Corp Ltd. v. Burroughs Business Machines Ltd et al.* (1977), 15 O.R.(2d) 750, 76 D.L.R.(3d) 641 (Ont. H.C.); *R. v. Biasi (No.2)* (1981), 66 C.C.C.(2d) 563 (B.C.S.C.); *R. v. McLarty (No. 3)* (1978), 45 C.C.C. (2d) 184 (Ont. Co. Ct.); *R. v. West*, [2001] O.J. 3413 (Ont. S.C.). Note that s. 30(10) CEA, and s. 42(4) B.C.E.A. exclude such records from being admissible as business record exceptions to the hearsay rule.

87 Compare, *R. v. McMullen*, 1979 CarswellOnt 1494, [1979] O.J. No. 4300, 25 O.R. (2d) 301, 47 C.C.C. (2d) 499, 100 D.L.R. (3d) 671 (Ont. C.A.), at p. 506 [C.C.C.] [*McMullen*], with, *R. v. Vanlerberghe* (1976), 6 C.R. (3d) 222 (B.C. C.A.) [*Vanlerberghe*]; note the difference when expert testimony is used as in *Vanlerberghe*. However, it is an open question as to whether evidence of "system integrity" in satisfaction of the electronic record provisions, would be sufficient to prove the "usual and ordinary course of business." A system having such "integrity" would make its records "in the usual and ordinary course of business," but the converse would not necessarily be true.

88 *R. v. Felderhof*, 2005 ONCJ 406, 201 C.C.C. (3d) 384, 2005 CarswellOnt 4726, [2005] O.J. No. 4151 (Ont. C.J.) [*Felderhof*]; *R. v. Laverty (No. 2)* (1979), 47 C.C.C. (2d) 60 (Ont. C.A.); *Robb v. St. Joseph's Health Care Centre*, [1999] O.J. 2003 (Ont. S.C.); *Catholic Children's Aid Society of Toronto v. J.L.* (2003), 39 R.F.L. (5th) 54, [2003] O.J. 1722 (Ont. S.C.); *Re S.V.*, [2002] S.J. No. 714 (Sask. Q.B.).

> poses of an "accuracy comparison" if called for.[89] Should electronic records have the same legal status as their paper originals if those originals are no longer available to verify the accuracy of those electronic descendants? And should printouts have the legal status of their electronic parents and ancestors after they have been deleted from their hard drives or other forms of electronic or optical storage?[90] Software now affects all three rules of admissibility "seamlessly" — the hearsay, best evidence, and authentication rules — and therefore there should be a single legal rule "seamlessly" determining the admissibility of the products of the application of such software in making and storing electronic records.

And, the electronic record provisions, added to the Evidence Acts beginning with ss. 31.1 to 31.8 CEA in 2000, have raised more questions about the business record provisions:

> Won't proof of "system integrity" under the electronic record provisions always satisfy the "usual and ordinary course of business" test in the business record provisions as well, *i.e.*, can a records system still have the necessary "integrity" even though some or all of its records are not created "in the usual and ordinary course of business"?
>
> Will the "circumstances of the making test" in s. 30(6) CEA, s. 35(4) OEA, and s. 23(4) NSEA, be altered in meaning or usage by the enactment of the electronic record provisions; *i.e.*, these subsections allow an evaluation of any particular factor in the making of an electronic record in determining what "weight" to give it, and in the case of s. 30 CEA, whether it is admissible; is this not similar to the "system integrity test" of the electronic record provisions? Is it compatible with the nature of the hearsay rule and the best evidence rule that a "circumstances of the making test" be attached to a hearsay rule exception, but a "systems integrity test" be attached to a best evidence rule exception?
>
> Should the "relied upon printout" be subject to the business record provisions? It is created by the electronic record provisions (s. 41.4(3) AEA, s. 34.1(6) OEA; s. 23D(2) NSEA; s. 31.2(2) CEA) to be, "the record for purposes of the best evidence rule," if it has been, "manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on" it [the printout]. Should it also have to be proved to have been made, "in the usual and ordinary course of business," in order to use it in

---

89 Compare, *R. v. McMullen*, 1979 CarswellOnt 1494, [1979] O.J. No. 4300, 25 O.R. (2d) 301, 47 C.C.C. (2d) 499, 100 D.L.R. (3d) 671 (Ont. C.A.), with, *R. v. Bell and Bruce* (1983), 35 O.R.(2d) 164 at 166; 65 C.C.C.(2d) 377 at 380 (OCA); affirmed without reasons [1985] 2 SCR 281, 55 O.R.(2d) 287.

90 The electronic record provisions deal with this issue, but in relation to the best evidence rule, not the hearsay rule. And, they merely state that, "in relation to an electronic record the best evidence rule is satisfied on proof of the integrity of the electronic record system." They say nothing about the effects of the destruction of original paper records or of the destruction of electronic versions of paper printouts. Can the electronic records system have the necessary "integrity" in relation to those records after such destruction?

> proof of the truth of some fact stated in it?[91]
>
> The British Columbia *Evidence Act* does not yet contain electronic records provisions (other than its "electronic court documents," ss. 41.1 to 41.4). Will the interpretation and use of its business record provisions therefore be different than in proceedings subject to an *Evidence Act* having both sets of provisions? And the Newfoundland and Labrador *Evidence Act* also awaits electronic records provisions. But the courts in B.C. and Newfoundland and Labrador didn't before, and are therefore unlikely now to hold electronic records to be inadmissible.

Such unanswered "hearsay" questions could be resolved by statute to allow the business record provisions to be compatible with the electronic records provisions of the Evidence Acts.[92]

VII. ELECTRONIC DISCOVERY

To effect the usage of existing legislation advocated above, requires adequate and principled electronic discovery applicable in both criminal and civil proceedings — entitlements under the rules of evidence are useless without the appropriate productions from disclosure and discovery with which to use those rules. The proponent of any electronically written or stored information should have to make discovery of all aspects of the electronic records system at issue. Admissibility under

---

91 The business record subsections, s. 30(11) CEA, s. 35(5) OEA, and s. 23(5) NSEA, state that those sections do not affect the operation of any other rule of admissibility. Therefore one could use the common law business record exception to the hearsay rule if admissibility cannot be obtained under these sections. Or, one could use the "principled approach to the rule against hearsay evidence" declared in, *R. v. Starr*, 2000 SCC 40, 2000 CarswellMan 449, 2000 CarswellMan 450, [2000] S.C.J. No. 40, [2000] 2 S.C.R. 144, 147 C.C.C. (3d) 449, 190 D.L.R. (4th) 591, [2000] 11 W.W.R. 1 (S.C.C.) [*Starr*], which holds *inter alia*, that written statements may be admitted in proof of the truth of their contents if "reliable and necessary," even though they may not be admissible under a traditional exception of the hearsay rule. The Supreme Court modified its decision in *Starr* in *R. v. Khelawon*, 2006 SCC 57, 2006 CarswellOnt 7825, 2006 CarswellOnt 7826, [2006] S.C.J. No. 57, [2006] 2 S.C.R. 787 (S.C.C.) [*Khelawon*], holding that the factors in regard to admissibility are not to be separated into "threshold and ultimate reliability" factors, but are to be considered together. The application of the "principled approach" is exemplified for records as admissible hearsay evidence by, *R. v. Wilcox*, 2001 CarswellNS 83, [2001] N.S.J. No. 85, 152 C.C.C. (3d) 157, 192 N.S.R. (2d) 159, ¶59 to 76 (N.S. C.A.), [*Wilcox*].

92 A contrary opinion as to the state of hearsay issues attendant to electronic records is given by John D. Gregory, in, "Canadian Electronic Commerce Legislation," (2002), 17 Banking & Finance Law Review (Carswell) 277, at 328 *et seq.*, (see: http://pages.ca.inter.net/~euclid1/bflr2002.pdf (at p. 20 *et seq.*)) whereat the author states: "The rules on hearsay are generally accepted to present no special problems for the admission of electronic records." For further quotation from, and analysis of this article, see: Ken Chasse, "Electronic Records as Documentary Evidence," (2007), 6 Canadian Journal of Law and Technology 141, note 109 and accompanying text in part 10, "Answering John Gregory's Attack." And in regard to John Gregory himself, see also notes 28, 50, and 91 in that CJLT article.

the electronic records provisions puts an electronic records system's "systems integrity" at issue, and not just that of one of its records adduced as evidence, nor just that part of the RM system where the record was recorded or stored. If such level of discovery is not performed, the court should not admit the evidence because the hearing as to "system integrity" could not in fairness proceed, nor provide adequate assurance of such "integrity."

As aptly stated by Judge Shira A. Scheindlin, U.S. District Judge, Southern District of New York:[93]

> Despite the changes in discovery practice resulting from the era of electronic record-keeping, the purpose of discovery remains unchanged. Discovery continues to be the key component in the search for truth. Liberal discovery is at the heart of the effective administration of justice in the United States. To that end, counsel's duty to both seek and provide discovery has not changed. Judges have little tolerance for attorneys (and litigants) who do not give serious attention to their discovery obligations. Failure to preserve, or to collect and review relevant information, may lead to the absence of critical evidence, which defeats the truth-seeking process.

Particularly so in criminal proceedings, such discovery is essential to the proper operation of the records provisions of the CEA, and therefore must be much more than the fulfilling of an obligation by the prosecution to disclose and produce that which the Crown prosecutor believes is relevant to the defence, and within the Crown's "investigative file."[94] The practice in regard to electronic discovery is wider in civil proceedings even though the legal obligation is the same. The practice in criminal proceedings has a smaller scope because (1) it is limited to the contents of the "investigative file"; (2) limited to the Crown's determination of what is relevant; and, (3) by the belief that third party claims as to the intellectual property law protections, privileges, trade secrets, and proprietary rights justify the Crown's taking the position that such evidence is beyond its control. Therefore beyond its disclosure obligation, and therefore the defence can chose to pursue it by way of an *O'Conner-McNeil* application.[95] No party should be able to use evidence

---

93 Writing in the "Forward," p. X, of, Michele C.S. Lange and Kristin M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now* (American Bar Association Publishing, 2009). Judge Scheindlin is an advisory board member of the Sedona Conference, and served on the Advisory Committee on Civil Rules, which proposed the 2006 Amendments to the (U.S.) Federal Rules of Civil Procedure.

94 As to the disclosure and discovery obligations upon the Crown in relation to the "investigative file," see note 7 *supra*.

95 The decisions of the Supreme Court of Canada in *O'Connor* and *McNeil* are cited *ibid*. Clearly the concept of "the contents of the investigative file" as defining the extent of the prosecutor's disclosure obligation in Canada is now well entrenched, judicially as well as in practice. Therefore that "file," in concept as well as in practice, will have to be expanded to make electronic discovery effective to the defence and to the fulfillment of the prosecutor's obligations to the defence in criminal proceedings. See: Ken Chasse, "Electronic Discovery in the Criminal Court System" (2010), 14 Canadian Criminal Law Review 111. It is an inadequate concept because it delivers to the defence at the very most, only that which is of interest to the police, leaving to the defence to bring an *O'Connor-McNeil* application for further disclosure. Such motion is

in regard to which adequate electronic discovery has not been made.

Nor can any argument be entertained that the courts just don't have time for the time-consuming complexities of electronic discovery. "Make discovery or don't use the evidence," should be a key tenant of discovery, and a condition-precedent to admissibility. Otherwise, evidence without opportunity to challenge it operates with an unjustified presumption of reliability which, if it relates to essential issues, can in effect reverse the presumption of innocence guaranteed by Charter of Rights s. 11(d).[96]

American commentators, although disagreeing on how to adjust the admissibility rules best to cope with electronic records, all agree that (1) adequate electronic discovery is critical to their use as evidence; and, (2) electronic discovery is itself a major area of law and legal practice, and not just an adjunct procedure in the service of litigation. That it is, but it is many times more complex, costly, time-consuming, and important than traditional, non-electronic discovery. For example, as a result, important amendments were made to the U.S. Federal Rules of Civil Procedure (FRCP) to accommodate electronic discovery of electronically stored information (ESI). They are summarized in the 2008 New York University Annual

---

seriously hobbled by lack of access to third party databases, and lack of knowledge of what to ask for in prescribed detail. For example, a thorough search for relevant electronic data and records should involve many and diverse electronic locations such as: business and home computers, laptop and desktop; FTP servers; email servers; CD's; hard drives; fileservers; floppy disks; remote storage; PDA's; web servers; backup tapes; blackberries (or competitors); digital cameras; thumbdrives; digital fax machines; and retired computers and other electronic devices. Can such a "rolled up blanket request" be successful without further detail supporting claims that such sources are likely to contain relevant evidence and information?

96 Evidence that cannot be challenged as to its accuracy and reliability will be presumed to be correct, and therefore, as it relates to key issues in a trial, will have the effect of reversing the burden of proof. That was one of the key points emphasized by the *Goudge Inquiry Report*, being the, *Inquiry into Pediatric Forensic Pathology in Ontario Report, Volume 3: Policy and Recommendations*, The Honourable Stephen T. Goudge, Commissioner, September 30, 2008 (Ontario Ministry of the Attorney General, Queen's Printer Ontario, 2008), online: for one year after publication at: <www.goudgeinquiry.ca>, and thereafter: <www.attorneygeneral.jus.gov.on.ca>

The inquiry was prompted by the work of a pediatric forensic pathologist whose incompetent opinions and testimony resulted in wrongful convictions. See the references to Justice Goudge's *Report*, and to the contrasting approach to disclosure and discovery in the *LeSage-Code Report* (the first, a response to wrongful convictions; the second, a competing response to demands for greater efficiency), in, Ken Chasse, *Electronic Discovery in the Criminal Court System*, (2010), 14 Canadian Criminal Law Review 111. The *LeSage-Code Report* by, Honourable Patrick J. LeSage, C.M. Q.C., (former Chief Justice of the Ontario Superior Court of Justice), and Professor Michael Code, (Faculty of Law, University of Toronto), *Report of the Review of Large and Complex Criminal Case Procedures*, submitted to the Honourable Chris Bentley Attorney General of Ontario, November 2008 (Queen's Printer for Ontario: Ontario Ministry of the Attorney General, 2008), online: <www.attorneygeneral.jus.gov.on.ca>

Survey of American Law as follows:[97]

> Then, in 2006, amendments to the FRCP changed the Rules in six key areas: (1) ESI became a separate category of discovery materials; (2) the FRCP mandated early attention to e-discovery issues; (3) new rules created a separate procedure for ESI that was "not reasonably accessible"; (4) new rules were adopted to allow parties to assert privileges after production; (5) Rules 33, 34 and 45 were revised to apply to ESI, including the form of production; and (6) Rule 37 set forth a "safe harbour" for ESI lost as a result of the "routine, good-faith operation of an electronic information system." . . . [*e.g.*], the party produced a privileged memorandum from a database that it believed contained only non-privileged documents. . . . A common issue regarding the form of production is whether the producing party shall be required to produce metadata. The good faith requirement of Rule 37 means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. Because emails often contain a combination of idle chatter, party admissions, and hearsay, parties must be precise about which parts of emails constitute business records.

Alterations have also been made to Canadian statutory law to accommodate electronic discovery. For example, the *Sedona Canada Principles — Addressing Electronic Discovery*, for civil proceedings[98] are being applied across Canada,[99]

---

97 Emily Burns, Michelle Greer Galloway, and Jeffrey Gross, "E-Discovery: One Year of the Amended Federal Rules of Civil Procedure," (2008), 64 N.Y.U. Ann. Survey. Am. L. 201, at 201 [2008 New York University Annual Survey of American Law].

98 *The Sedona Canada Principles — Addressing Electronic Discovery*, online: The Sedona Conference, Canada, January 2008: <http://www.thesedonaconference.com/content/miscFiles/canada_pincpls_FINAL_108.pdf> or, <http://www.thesedona conference.org/dltForm?did=canada_pincpls_FINAL_108.pdf> and, online: E-Discovery Canada website, hosted by LexUM (at the University of Montreal), online: <http://www.lexum.umontreal.ca/e-discovery>

Hereinafter "*Sedona Canada Principles"* because there are *The Sedona Principles Addressing Electronic Document Production*, Second Edition (June, 2007) applicable in the U.S., also available from the Sedona Conference website, online: <http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf>

In addition, in July 2008, the Sedona Conference launched its "Cooperative Proclamation," described as, "a coordinated effort to promote cooperation by all parties in the discovery process to achieve the goal of a 'just, speedy, and inexpensive determination of every action'." . . . "Only when lawyers confuse *advocacy* with *adversarial conduct* are these twin duties in conflict" (*i.e.*, the duties of being zealous advocates for their clients, and a professional obligation to conduct discovery with integrity and in a diligent, candid manner. See: http://www.thesedonaconference.org/content/tsc_cooperative_proclamation/proclamation.pdf

99 For example, the following recent decisions apply or cite as a recognized standard the *Sedona Canada Principles*: *Dykeman v. Porohowski*, 2010 BCCA 36, 2010 CarswellBC 136, [2010] B.C.J. No. 113, 1 B.C.L.R. (5th) 246 (B.C. C.A.); *Innovative Health Group Inc. v. Calgary Health Region*, 2008 ABCA 219, 2008 CarswellAlta 736, [2008] A.J. No. 615, ¶26 (Alta. C.A.); additional reasons at 2008 CarswellAlta

and they have been incorporated by reference into the Ontario *Rules of Civil Procedure* — Rule 29.1.03(4).[100] Other authoritative guidelines have been declared in various provinces.[101]

Electronic RM, discovery, and rules of evidence are now a mutually interdependent whole. But for the most part, civil litigation favours discovery over the rules of evidence, and criminal, the opposite. In fact, electronic discovery and the rules of evidence are interdependent. They are not mutually exclusive, nor alternative tools.

All of the above indicates this very important fact for litigation lawyers, in order to cope with both the admissibility of electronic records and related discovery procedures and motions for production, they have to become more knowledgeable

---

982 (Alta. C.A.); leave to appeal refused 2008 CarswellAlta 1819, 2008 CarswellAlta 1820 (S.C.C.); *Doucet v. Spielo Manufacturing Inc.*, 2007 NBCA 85, 2007 CarswellNB 551, 2007 CarswellNB 552, [2007] N.B.J. No. 510, ¶11 (N.B. C.A.); *Saint John (City) Employee Pension Plan v. Ferguson*, 2009 NBQB 74, 2009 CarswellNB 128, [2009] N.B.J. No. 92, ¶15-16 (N.B. Q.B.); *Vector Transportation Services Inc. v. Traffic Tech Inc.*, 2008 CarswellOnt 1432, [2008] O.J. No. 1020, ¶19 (Ont. S.C.J.); additional reasons at 2008 CarswellOnt 2540 (Ont. S.C.J.); *Commonwealth Marketing Group Ltd. v. Manitoba (Securities Commission)*, 2008 MBQB 319, 2008 CarswellMan 602, [2008] M.J. No. 430, ¶7 (Man. Q.B.); affirmed 2009 CarswellMan 94 (Man. C.A.); *Borst v. Horizon Financial Group Inc.*, 2009 CarswellOnt 5984, [2009] O.J. No. 4115, ¶3 (Ont. Master), Master R. Brott; *Andersen v. St. Jude Medical Inc.*, 2008 CarswellOnt 6654, [2008] O.J. No. 430, ¶27 and 28 (Ont. Master), Master C.U.C. MacLeod.

100 Rule 29.1.03(4): "In preparing the discovery plan, the parties shall consult and have regard to the document titled 'The Sedona Canada Principles Addressing Electronic Discovery' developed by and available from The Sedona Conference. O. Reg. 438/08, s.25." (Operative from January 1, 2010) The new rules concerning discovery plans are published in, James J. Carthy, W.A. Derry Millar & Jeffrey G. Cowan, *2009-2010 Ontario Annual Practice* (Aurora, Ontario: Canada Law Book, 2009) at 576, and 893-894.

101 *Ontario*: *Guidelines for the Discovery of Electronic Documents in Ontario* (November, 2005), online: Ontario Bar Association <http://oba.org/en/pdf_newsletter/E-DiscoveryGuidelines.pdf>

Alberta: see the, *Court of Queen's Bench of Alberta Civil Practice Note No. 14 — Guidelines for the Use of Technology in Any Civil Litigation Matter*, May 30, 2007; and the *Alberta Generic Protocol Document*, online: <http://www.albertacourts.ab.ca/qb/practicenotes/civil/pn14technology.pdf>

and: <http://www.albertacourts.ab.ca/qb/practicenotes/civil/pn14-protocol.pdf>

They are reproduced in, Todd J. Burke *et al.*, *E-Discovery In Canada* (LexisNexis Canada Inc., 2008), Appendices 7 and 8, pp.231–270.

British Columbia: see the, *British Columbia Supreme Court Practice Direction re Electronic Evidence*, July 1, 2006, and the, *British Columbia Generic Protocol Document*, reproduced in, Todd J. Burke *et al.*, *E-Discovery In Canada* (LexisNexis Canada Inc., 2008), Appendices 5 and 6, pp.193–230.

All of the above need compliance with the National Standards of Canada for electronic records management to work properly; see: notes 36, 40, 46, and 50 *supra* and accompanying text.

about RM principles and practices. Under the heading, "Unique Challenges of Electronic Discovery," an American attorney tells why lawyers have to become more knowledgeable about electronic information systems:[102]

> E-discovery presents a new series of challenges which require attorneys to understand their clients' and adversaries' information systems. There is a wide variety of types of digital data which has to be considered in e-discovery, such as: e-mails, data compilations, drafts, electronically created and stored documents, pictures, audio files, voicemails, Internet use records, and much more. This wide variety of electronic data resides on networks, computers and portable devices, often with multiple copies in different locations. Servers and network appliances often contain substantial information about how the network has been used, such as: access to systems (logons/logoffs), access to programs/files, use of printers, faxes, etc., e-mail use and Internet use. Data is also frequently copied to backup media like backup tapes and mirror servers. This list is likely to continue to grow with advances in technology.
>
> The E-Discovery Process Includes the Following Steps; 1. Preservation; 2. Collection; 3. Processing (including filtering, dedulication, maintaining relationships between records, etc.); 4. Reviewing; 5 Producing. Service providers can perform these steps or assist attorneys in performing them. It is, of course, necessary for attorneys to participate in reviewing for relevancy and privilege. Service providers utilize powerful search tools, like conceptual searching, and provide hosting for large volumes of data which can be viewed and processed over the Internet.

Note that the articles cited herein show (1) not only an understanding of the close relationship between knowledge of RM principles and practices and the new laws and analytical approaches to electronic discovery and the admissibility of evidence; but also therefore, (2) an understanding of the interdependent relationship between the FRE and the new Federal Rules of Civil Procedure for electronic discovery. Changes to either will cause changes to the other, in both content or interpretation. Canadian lawyers have some catching-up to do. Criminal lawyers have a long way to go.[103]

---

102 David G. Ries, "Records Management: Current Issues in Retention, Destruction, and E-Discovery," (2007), 78 PA Bar Assn. Quarterly 139. David G. Ries is a partner in the Pittsburgh office of Thorp Reed & Armstrong, LLP. This article explains why American attorneys have to become more knowledgeable about records management principles and practices. And it describes the electronic discovery process.

103 On this topic of the absence of electronic discovery procedures in Canadian criminal law, and of an understanding of them and of the need for them, see: Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111. Obligations regarding the safekeeping of electronic records and other records when litigation is pending is itself a complicated RM subject involving the identification, preservation, collection, review (for relevance, and privilege, privacy, and confidentiality), and production of relevant records. A "litigation hold" program should be designed and documented within the records policy and procedures manual before litigation is contemplated and discovery request letters are received. This follows from the acceptance by Canadian courts of this key "discovery" proposition: "once a party reasonably anticipates litigation, it must suspend its routine retention-

That critical interdependence of evidence and discovery (*i.e.*, disclosure, production, and discovery), which is standard procedure in civil proceedings, is lacking in criminal proceedings in Canada. Defence and Crown counsel should operate according to these principles:

> 1. Prosecution is defence; defence is offence, *i.e.*, the Crown prosecutor's strategy in a criminal trial is to protect its case. Defence strategy is most often to attack the Crown's case.
>
> 2. Discovery and admissible evidence are interdependently linked. The complexities of electronically stored information make the defence increasingly dependent upon the Crown for defence evidence and strategies of defence. (Such dependence is aggravated by the limitations of Legal Aid.)
>
> 3. The credibility of electronically-produced evidence is the same as the credibility of a witness — it is of one whole piece. But the defence asks only for copies of the records to be adduced by the Crown. Defence counsel should also be asking for disclosure of the Crown's method of proving, "the integrity of the electronic documents system by or in which the electronic document was recorded or stored." Those words in s. 31.2(1)(a) CEA mean that the admissibility of an electronic document is dependent upon proof of the "integrity" (credibility) of the whole electronic documents system, not just that part that produced, stored, or otherwise "touched or concerned" the record.
>
> 4. The Crown's current practice in regard to discovery is determined by that of the defence, *i.e.*, if the defence is undemanding and satisfied with a low standard of discovery, that will determine the Crown's practice. In addition, the Crown's practice should be shaped by its obligations to the accused, to ensuring that innocent accused persons are not convicted, and that those convicted are convicted properly and in good conscience.

---

destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); 2003 U.S. Dist. LEXIS 18771 (*Zubulake IV*), being a case much cited in Canada, and recently updated in, *The Pension Committee of the University of Montreal Pension Plan, et al. v. Banc of America Securities, LLC, et al.*, 2010 WL 184312 (S.D.N.Y. Jan. 11, 2010) (U.S. District Court, Southern District of New York) concerning the "sanctions" appropriate for gross negligence in the performance of electronic discovery. And, *Sedona Canada* Principle 3: "As soon as litigation is reasonably anticipated, parties must consider their obligation to take reasonable and good faith steps to preserve potentially relevant electronically stored information." Note also that organizations should also have a similar "tax hold" procedure that operates when notified of a government tax "assessment." In addition, good RM procedure will require that there be a "document hold" that is long enough to provide for: (1) quality control inspection; (2) business unit processing; and, (3) audit requirements. Typically, this "document hold" period may vary from two to six months, based upon the business unit processing cycle and the system "secured storage" and audit functions. These points can be used in cross-examination, and as reasons for not accepting superficial, uninformed excuses for failure to make adequate discovery.

> Crown counsel should guard against being "wilfully blind" to the nature and quality of the record systems that produce relevant evidence, *i.e.*, not be content with what the police give and say about their sources.
>
> 5. Therefore, the *O'Connor-McNeil* application is an inadequate procedure for the needs of discovery for the defence, and an inadequate answer by the Crown to defence requests for discovery.[104]

This critical interdependence of evidence and discovery in criminal proceedings has been dealt with in more detail elsewhere, along with their relationship to electronic RM.[105]

VIII. CHARTER RIGHTS AND ADMISSIBILITY

Admissibility requires decisions on the authenticity of electronic records and the "reliability" of the systems they come from. Software and its electronic devices are perfected only to the point of marketability, not infallibility. Court decisions based upon the evidence produced by electronic devices, if not subjected to a sufficiently high and thorough "threshold of admissibility," in effect allow those devices to displace laws establishing the respective burdens and onuses of proof of civil and criminal liability, with the standards of success in the marketplace. For criminal proceedings, that fact violates constitutional rights as to, "fundamental justice," "full answer and defence," "fair trial," "an independent and impartial tribunal," and, "proof beyond a reasonable doubt."[106] And they similarly displace constitu-

---

104 See: *R. v. McNeil*, 2009 SCC 3, 2009 CarswellOnt 116, 2009 CarswellOnt 117, [2009] S.C.J. No. 3, [2009] 1 S.C.R. 66 (S.C.C.) [McNeil] at para.42; *R. v. Shearing*, 2002 SCC 58, [2002] 3 S.C.R. 33, 165 C.C.C. (3d) 225, 2 C.R. (6th) 213 (S.C.C.) [*Shearing*]; *R. v. Mills*, [1999] 3 S.C.R. 668, 139 C.C.C. (3d) 321, 28 C.R. (5th) 207, 180 D.L.R. (4th) 1 (S.C.C.) [*Mills*]; *R. v. O'Connor*, 1995 CarswellBC 1098, 1995 CarswellBC 1151, [1995] S.C.J. No. 98, [1995] 4 S.C.R. 411, 103 C.C.C. (3d) 1 (S.C.C.) [*O'Connor*]; *R. v. Chaplin* (1994), [1995] 1 S.C.R. 727, 96 C.C.C. (3d) 225 (S.C.C.) [*Chaplin*]; *R. v. Stinchcombe*, 1991 CarswellAlta 559, 1991 CarswellAlta 192, [1991] S.C.J. No. 83, [1991] 3 S.C.R. 326, 68 C.C.C. (3d) 1 (S.C.C.) [*Stinchcombe*]; *R. v. Bjelland*, 2009 SCC 38, 2009 CarswellAlta 1110, 2009 CarswellAlta 1111, [2009] S.C.J. No. 38 (S.C.C.) [*Bjelland*].

105 See: Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111.

106 The right, "to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal," is guaranteed by s. 11(d) of the Canadian Charter of Rights and Freedoms to, "any person charged with an offence." Rights as to, "an opportunity to make full answer and defence" and to "fundamental justice" are entrenched within Charter s. 7 ("Everyone has the right to life, liberty, and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."). Rights as to "fair trial" and "proof beyond a reasonable doubt" are entrenched within Charter s. 11(d). The Canadian Charter of Rights and Freedoms, being Part 1 of the *Constitution Act, 1982*, *Canada Act 1982* (U.K.), c. 11 R.S.C. 1985, Appendix II, No. 44, as amended, proclaimed in force April 17, 1982 ((hereinafter, "the Charter" or, "Charter of Rights"). Its drafting drew heavily from the experience of the American Bill of Rights (the first ten Amend-

tional rights in civil proceedings where "state action" is involved.[107]

Therefore, such constitutional rights are very much dependent upon the evidentiary rules that determine the admissibility and "weight" of evidence produced by electronic technology, particularly most frequently electronic records. If those rules are sufficient to guarantee the availability of such constitutional rights, then the standards of the marketplace will not be able to displace the operation of laws establishing the burdens and onuses of proof of civil and criminal liability.

As argued above, the "usual and ordinary course of business" test of the business record provisions is an inadequate guarantee of accurate records for evidentiary purposes.[108] Those business records are almost always produced by and stored in electronic RM systems that depend upon uncertified electronic equipment and software. Therefore, the "usual and ordinary course of business" test needs to be supplemented by, and more appropriately, "led by" (1) the "systems integrity test" of the electronic records provisions; and, (2) the "circumstances of the making" test (an exclusionary rule of the s. 30(6) CEA type, as argued above).

But what effect does the new "principled approach to the rule against hearsay evidence" (*i.e.*, a new hearsay rule exception) have upon (1) the existing, traditional exceptions to the hearsay rule, such as the exception at common law for business records "made in the routine of business"[109]; and, (2) statutory exceptions, such as

---

ments of the U.S. Constitution). But its interpretation has taken the law significantly elsewhere, mainly because of differences in legal history and tradition, and political culture.

107 The Charter of Rights, *ibid.*, applies only to the actions of the state ("state action"), particularly those of agents of the state such as police officers, hospitals, universities, and Legal Aid agencies.

108 The electronic record systems of even very good private and public sector organizations may have many defects of quantity and quality and nonetheless be sufficiently successful in the marketplace, the stock market, and in the world of public (political and parliamentary) accountability. But that success cannot displace or compensate for the fact that such defects undermine the credibility of any particular record adduced as evidence. See the list of defects above in section 4, "The Common Defects of RM Systems Affect Admissibility and 'Weight'." "Macro success" in business or other enterprise, does not require "micro integrity." But such success should not dictate the content of "system integrity," nor the burden of proof.

109 For an analysis of this common law hearsay rule exception, see: (1) Ken Chasse, "Electronic Records As Documentary Evidence," (2007) 6 Canadian Journal of Law and Technology" 141 (the exception is analyzed at several places in the article); (2) J. Douglas Ewart, *Documentary Evidence In Canada* (Toronto: Carswell; 1984)., p. 53, whereat the author provides a comparative list of the constituent elements of the common law rule, and the "Impact of *Ares*" [*Ares v. Venner*, [1970] S.C.R. 608, 14 D.L.R. (3d) 4, 12 C.R.N.S. 349 (SCC)] upon each of the constituent elements of the common law rule by way of a comparative listing of the "Traditional Rules" that made up the common law hearsay exception before *Ares* (in left hand column) with the "Impact of Ares" upon each of them (in the right hand column); (3) a useful discussion of these points can also be found in the, *Report of the Federal/Provincial Task Force on Uniform Rules of Evidence*, (Toronto: Carswell; 1982) at pp. 390–401 (being ss. 29.11 & 29.12 of the *Report*), and elsewhere whereat the decision in *Ares v. Venner*, *supra*, is discussed; (4) in the context of criminal proceedings and generally in relation to the

the business record provisions of the Evidence Acts? In *R. v. Starr* (S.C.C., 2000)[110] the Supreme Court of Canada held that hearsay evidence that cannot meet the "necessity" and "reliability" tests of the "principled approach to the admissibility of hearsay evidence," must be excluded, even though such hearsay comes within an established exception to the hearsay rule. And conversely, it can be admitted if it satisfies those tests even though it does not come within an established exception. The "reliability" test can be argued to require an examination of the records system that generated the record. Although the analysis in *Starr* concerned the "traditional exceptions" to the hearsay rule and not statutory exceptions such as the business record provisions of the Evidence Acts, it can be argued that *Starr* is equally applicable to statutory exceptions. Note also that the statutory business record exceptions contain a provision stating that such exception does not derogate from the admissibility of a record under any other rule of law.[111] The majority judgement of Iacobucci J., as he then was, contains the following paragraphs (199–201) that link the "principled approach" to the Canadian Charter of Rights and Freedoms[112]:

> Why the Exceptions Must be Rationalized
>
> [199] As I have already discussed, a fundamental concern with reliability lies at the heart of the hearsay rule. By excluding evidence that might produce unfair verdicts, and by ensuring that litigants will generally have the opportunity to confront adverse witnesses, the hearsay rule serves as a cornerstone of a fair justice system.
>
> [200] In *Khan*, *Smith*, and subsequent cases, this Court allowed the admission of hearsay not fitting within an established exception where it was sufficiently reliable and necessary to address the traditional hearsay dangers. However, this concern for reliability and necessity should be no less present when the hearsay is sought to be introduced under an established exception. This is particularly true in the criminal context given the "fundamental principle of justice, protected by the Charter, that the innocent must not be convicted": *R. v. Leipert*, [1997] 1 S.C.R. 281, ¶24, 112 C.C.C. (3d) 385, 143 D.L.R. (4th) 38 quoted in *R. v. Mills*, [1999] 3 S.C.R. 668, ¶71, 139 C.C.C. (3d) 321, 180 D.L.R. (4th) 1. It would compromise trial fairness, and raise the spectre of wrongful convictions, if the Crown is allowed to intro-

---

Canada Evidence Act, see: E.G. Ewaschuk, *Criminal Pleadings and Practice in Canada*, 2nd ed. (Toronto: Canada Law Book, 2009), at para. 16:15110, "Business records"; and, (5) the "progeny of *Ares*" (case law produced by *Ares v. Venner*, *supra* note 2) should also be analyzed, for it remains today the leading decision defining the common law exception for business records in Canada.

110 *R. v. Starr*, 2000 SCC 40, 2000 CarswellMan 449, 2000 CarswellMan 450, [2000] S.C.J. No. 40, [2000] 2 S.C.R. 144, 147 C.C.C. (3d) 449, 190 D.L.R. (4th) 591, [2000] 11 W.W.R. 1 (S.C.C.) [*Starr*].

111 See for example: s. 30(11) CEA; s. 35(5) OEA; s. 23(5) NSEA; (the *Alberta Evidence Act* and that of Newfoundland and Labrador have no business record exception, and thus remain dependent upon that at common law, as defined in, *Ares v. Venner* (S.C.C., 1970), *supra* notes 2, 21, and 109, and accompanying text).

112 Being Part I, *Constitution Act, 1982*, enacted by the *Canada Act 1982* (U.K.), c. 11 R.S.C. 1985, Appendix II, No. 44, proclaimed in force April 17, 1982.

> duce unreliable hearsay against the accused, regardless of whether it happens to fall within an existing exception.
>
> [201] In addition to improving trial fairness, bringing the hearsay exceptions into line with the principled approach will also improve the intellectual coherence of the law of hearsay. It would seem anomalous to label an approach "principled" that applies only to the admission of evidence, not its exclusion. Rationalizing the hearsay exceptions into the principled approach shows that the former are simply specific manifestations of general principles, rather than the isolated "pigeon-holes" referred to in U. (F.J.), *supra*, at para. 20.

The "principled approach to hearsay evidence" has thus been made a constitutional principle of trial fairness. Therefore it is superior to any statutory provision such as the record and document provisions of the Evidence Acts. Therefore the inadequacy of their "usual and ordinary course of business" test can be displaced (or supplemented) by the "reliability and necessity" requirements of the "principled approach to hearsay evidence." But, being a "Charter fair trial" argument such "displacement" would be applicable only in criminal proceedings, and other proceedings where "state action" is connected to evidentiary issues.[113] It can therefore be used to request an examination of the reliability of a record, and therefore of the record system it comes from, whether or not the application of s. 30 CEA results in a finding of that record's admissibility or inadmissibility. Thus the "principled approach" is superior to both common law and statutory exceptions to the hearsay

113 The "fair trial" provision of the Canadian Charter of Rights and Freedoms, s. 11(d), applies only to, "Any person charged with an offence." And, the Charter applies only to "state action," which is not relevant in most civil proceedings. Therefore, the s. 7 "fundamental justice" and "full answer and defence" provisions would not be available unless "state action" were involved; *e.g.*, a children's aid society taking custody of a child, or medical treatment for one's child; *B. (R.) v. Children's Aid Society of Metropolitan Toronto*, [1995] 1 S.C.R. 315 (S.C.C.); how to educate one's children, *R. v. Jones*, 1986 CarswellAlta 181, 1986 CarswellAlta 716, [1986] S.C.J. No. 56, [1986] 2 S.C.R. 284, 28 C.C.C. (3d) 513 (S.C.C.); a hospital failing to provide a sign language interpreter for communications between a doctor and a hearing-impaired patient: *Eldridge v. British Columbia (Attorney General)*, 1997 CarswellBC 1939, 1997 CarswellBC 1940, [1997] S.C.J. No. 86, [1997] 3 S.C.R. 624 (S.C.C.); timely access to health care: *Chaoulli c. Québec (Procureur général)*, 2005 SCC 35, 2005 CarswellQue 3276, 2005 CarswellQue 3277, [2005] S.C.J. No. 33, [2005] 1 S.C.R. 791 (S.C.C.); timely proceedings before a human rights commission, and administrative hearings in general: *Blencoe v. British Columbia (Human Rights Commission)*, 2000 SCC 44, 2000 CarswellBC 1860, 2000 CarswellBC 1861, [2000] S.C.J. No. 43, [2000] 2 S.C.R. 307 (S.C.C.); extradition of fugitives without obtaining assurances that the death penalty would not be imposed: *United States v. Burns*, 2001 SCC 7, 2001 CarswellBC 272, 2001 CarswellBC 273, [2001] S.C.J. No. 8, [2001] 1 S.C.R. 283 (S.C.C.); deportation of a refugee to face a substantial risk of torture: *Suresh v. Canada (Minister of Citizenship & Immigration)*, 2002 SCC 1, 2002 CarswellNat 7, 2002 CarswellNat 8, [2002] S.C.J. No. 3, [2002] 1 S.C.R. 3 (S.C.C.). Thus clearly s. 7 applies to civil cases as well as criminal cases. (*Charter* s. 7 states: "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.")

rule, where the Charter can be involved because "state action" is sufficiently connected to issues of admissibility. If the Charter cannot be so invoked, then the "principled approach" is nonetheless superior to the common law traditional exceptions, as established by the decision in *Starr*.[114] Therefore the common law business records exception, which requires a record "made in the routine of business," is subject to the "reliability and necessity" requirements of the "principled approach to hearsay evidence."[115]

However, this argument may be available only in regard to non-electronic records because proof of "system integrity," in compliance with the electronic record provisions of the Evidence Acts, should mean that the record intended to be used as evidence is reliable. But what of false information fed into an otherwise reliable electronic record system? Is the resulting record nevertheless admissible because it comes from an electronic record system having the required "system integrity"? Does proof of "system integrity" always require proof of the reliability of information fed into the electronic record system"? In those cases wherein the "principled approach to hearsay evidence" operates as a Charter of Rights principle, its "reliability" requirement would make the record inadmissible.

IX. COMPARING THE AMERICAN RULE: FEDERAL RULE OF EVIDENCE 803(6)

In contrast, the (US) Federal Rule of Evidence 803(6) expressly states that the hearsay rule does not exclude a "data compilation, in any form, . . . unless the source of information or the method or circumstances of preparation indicate lack

---

114 *Supra* note 105. The Supreme Court modified its decision in *Starr* in, *R. v. Khelawon*, [2006] S.C.J. No. 57, [2006] 2 S.C.R. 787, holding that the factors in regard to admissibility are not to be separated into "threshold and ultimate reliability" factors, but are to be considered together. The application of the "principled approach" is exemplified for records as admissible hearsay evidence by, *R. v. Wilcox*, 2001 CarswellNS 83, [2001] N.S.J. No. 85, 152 C.C.C. (3d) 157, 192 N.S.R. (2d) 159 (N.S. C.A.), [*Wilcox*], at paras. 59 to 76, and applied in, *R. v. Port Chevrolet Oldsmobile Ltd.*, 2009 BCCA 357, 2009 CarswellBC 2132, [2009] B.C.J. No. 1621 (B.C. C.A.); *R. v. Lemay*, 2004 BCCA 604, 2004 CarswellBC 2823, [2004] B.C.J. No. 2494, 191 C.C.C. (3d) 497 (B.C. C.A.) [*Lemay*].

115 Reasons for using the common law hearsay rule exception even though it is more onerous to satisfy than the *Evidence Act* exceptions, are: (1) it contains no notice provision; and, (2) it contains no prohibition as to "records made in contemplation of litigation" (as does s. 30(10) CEA, and s. 42(4) of the B.C. *Evidence Act*, R.S.B.C. 1996, c. 124). Therefore, even though a record is not admissible under s. 30 CEA or counterpart, it might be admissible under the common law exception: *R. v. Sunila*, [1986] N.S.J. No. 51; (1986), 26 C.C.C. (3d) 331 (N.S.S.C.). The statutory and common law business record exceptions can be used together, except in Alberta and Newfoundland and Labrador; their Evidence Acts do not contain a business records exception. As to the definition of the common law exception, see the references to *Ares v. Venner* (S.C.C., 1979), *supra* notes 2, 21, 109 and 111, and accompanying text.

of trustworthiness."[116] *McCormick on Evidence* states of this provision[117]:

> The theory of trustworthiness supporting the regularly kept records exception assumes a reliable method of entering, processing, storing, and retrieving data. Moreover, the rule excludes statements when "the source of information or the method or circumstances of preparation indicate lack of trustworthiness." Issues may arise at any of the stages of the handling of the data regarding (1) computer hardware, (2) software or programming, and (3) accuracy or security.

But the difference in concept upon which the Canadian electronic record provisions are based, and Rule 803(6), is stated by the same author on the same page:[118]

> While a well-laid foundation will touch upon each of the general areas noted above, the trend among courts has been to treat computer records like other business records and not to require the proponent of the evidence initially to show trustworthiness beyond the general requirements of the rule. The fact that the organization relies upon the record in the regular course of business may itself provide sufficient indication of reliability, absent realistic challenge, to warrant admission.

The Canadian concept does not treat electronic records as being like other business records. Secondly, the "system integrity" test could be interpreted as requiring in the first instance, more exact proof of trustworthiness than merely "general requirements." Rule 803(6) is a single business record provision dealing with both traditional paper and electronic records and systems, whereas the Canadian provisions deal with business records and electronic records in different provisions and therefore paper records and electronic records in different provisions — an elec-

---

116 Rule 803. Hearsay Exceptions: Availability of Declarant Immaterial

> The following are not excluded by the hearsay rule, even though the declarant is available as a witness:
>
> (6) Records of regularly conducted activity.
>
> A memorandum, report, record, or *data compilation*, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or *data compilation*, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, *unless* the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit. *[emphasis added]*

117 *McCormick on Evidence*, 6th edition (St. Paul MN: Thomson/West, 2006), at 497.

118 *Ibid.*

tronic business record must satisfy both. But in both the Canadian and American laws, the issues as to hearsay, best evidence, and authentication, are dealt with in separate provisions.[119]

X. WHAT DOES THE "SYSTEM INTEGRITY TEST" OF THE ELECTRONIC RECORDS PROVISIONS REQUIRE?[120]

The above analysis argues a need to interpret the electronic record provisions of the Evidence Acts as expanded "authentication" provisions of the American variety. That would provide a test of compliance with the "system integrity test." Then the "circumstances of the making" of the adduced record would be examined to determine if there is any reason to exclude it as not made "in the usual and ordinary course of business" of the business in question. The "circumstances of the making" subsections of the Evidence Acts would provide that necessary controlling function.[121] And thus "the usual and ordinary course of business" would not be allowed to set a "threshold of admissibility" that is far too low and undemanding of electronic records and the systems that produce them.

There is no helpful case law, but there is one decision that can be argued as providing guidance as to the meaning of the "system integrity test" in the electronic record provisions of the Evidence Acts. It is 31 years old: *R. v. McMullen* (Ont. C.A. 1979).[122] The electronic record provisions are now 10 years old. *McMullen* should have developed a line of cases that would have made the electronic record provisions unnecessary. Instead, it has been used merely to justify the use of electronically-produced records, but not to further the analysis as to what is required to make them admissible records.[123] *McMullen* is a s. 29 CEA banking records case,

---

119 The Federal Rules of Evidence provide a hearsay exception in Rule 803(6), and deal with best evidence rule and authentication issues in Rules 1001–1004 The Canadian business record provisions deal with all three types of issues for paper records in their business record sections, and deal with best evidence rule and authentication issues in their electronic record provisions. Hearsay issues for electronic records come within the business record sections or other record exceptions to the hearsay rule.

120 See note 29 *supra* for the words in the Evidence Acts giving rise to the "system integrity test." The whole of the electronic record provisions in the Evidence Acts of Alberta, Ontario, and Nova Scotia, and in the *Canada Evidence Act* are reproduced in Appendix C, below.

121 Provisions such as s. 35(4) OEA and s. 23(4) NSEA would have to be amended to allow such "circumstances of the making" of the record to go to admissibility as well as to "weight" (probative value; credibility). The bias favoring admissibility so as to leave rigorous assessment to "weight," that arose in the pre-computer law of evidence, is not justified in relation to electronic RM systems. The factual issues of such systems are too complex to be left: (1) entirely to a jury as the trier of fact and to issues as to "weight alone; and, (2) without adequate electronic discovery. Admissibility issues justify more directly the demands of electronic discovery — the burden of proof to be satisfied mandates discovery and production of the means of satisfying it.

122 [1979] O.J. No. 4300; (1979), 25 O.R. (2d) 301, 47 C.C.C. (2d) 499 at 506, 100 D.L.R. (3d) 671 (Ont. C.A.).

123 See for example, these "McMullen" cases — they cite it but don't develop its "McMullen standard" formulation for the admissibility of electronic records:

but it is a "best evidence rule" case, which is also the basis of the electronic record provisions. Therefore it is useful in interpreting those provisions. It defined what is now the "system integrity test" 31 years ago with these words:[124]

> The nature and quality of the evidence put before the Court has to reflect the facts of the complete record keeping process — in the case of computer records, the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation: see *Transport Indemnity Co. v. Seib* (1965), 132 N.W. 2d 871; *King v. State ex rel. Murdock Acceptance Corp.* (1969), 222 So. 2d 393, and 'Note, Evidentiary Problems and Computer Records', 5 Rut. J. Comp. L. 342 (1976), p. 355, et seq. If such evidence be beyond the ken of the manager, accountant or the officer responsible for the records (*R. v. McGrayne* (March 14, 1979) (Ontario Court of Appeal) [since reported 46 C.C.C. (2d) 63]) then a failure to comply with s. 29(2) must result and the print-out evidence would be inadmissible.[125]

The first sentence of this passage lays down a "systems test," as do the electronic record provisions, and it does so in words very similar to those used in those provisions. This "*McMullen* standard" is therefore a true forerunner of the "systems integrity test."

As to the necessary foundation evidence for the admissibility of electronic records, compare this "*McMullen* standard" with the "*Vinhnee*/Imwinkelried foundation" that American courts and commentators are now favouring, which requires proof of these 11 points:[126]

(1) the business uses a computer.

(2) the computer is reliable.

R. v. Cordell, [1982] A.J. No. 854 (Alta. C.A.);

R. v. Agyei, [2007] O.J. No. 391 (Ont. C.J.);

R. v. D.L.M., [1999] A.J. 1326, 141 C.C.C. (3d) 213 (Alta. Q.B.);

R. v. Daley, [2007] N.B.J. No. 443 (N.B. Provl. Ct.);

R. v. Lemay, [2004] B.C.J. 2494, 191 C.C.C. (3d) 497 (B.C.C.A.);

R. v. Marini, [2006] O.J. No. 4057 (Ont. S.C.J.);

R. v. Rideout, [2003] N.B.J. No. 217 (N.B. Provl. Ct.);

R. v. Tempest, [2002] O.J. No. 2467 (Ont. S.C.J.);

R. v. Tewolde, [2007] O.J. No. 4568 (Ont. C.J.).

124 *Supra* note 122, *infra* note 125; and, page 506, 47 C.C.C. (2d) 499.

125 The decision in *Bell and Bruce* further refined the use of *McMullen*, but it does not alter the meaning and importance of this passage — "the *McMullen* standard" as to the admissibility of electronically-produced business records: *R. v. Bell and Bruce*, [1982] O.J. No. 3116; (1982), 35 O.R. (2d) 164, 65 C.C.C. (2d) 377 (Ont. C.A.); affirmed [1985] S.C.J. No. 65, [1985] 2 S.C.R. 287, 55 O.R. (2d) 287n. For an analysis of this usage of *McMullen* see, Ken Chasse, "Electronic Records as Documentary Evidence," (2007) 6 Canadian Journal of Law and Technology 141, concerning this passage, "the *McMullen* standard."

126 *Supra* notes 67–76. This 11-point "*Vinhnee*/Imwinkelried foundation" test is quoted from para. 13 of the Cooper Offenbecher article, *supra* note 62.

> (3) the business has developed a procedure for inserting data into the computer.
>
> (4) the procedure has built-in safeguards to ensure accuracy and identify errors.
>
> (5) the business keeps the computer in a good state of repair.
>
> (6) the witness had the computer readout certain data.
>
> (7) the witness used the proper procedures to obtain the readout.
>
> (8) the computer was in working order at the time the witness obtained the readout.
>
> (9) the witness recognizes the exhibit as the readout.
>
> (10) the witness explains how he or she recognizes the readout.
>
> (11) if the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

This list is superficial and therefore inadequate for its professed purpose. It's a "lawyer's list" that identifies the complexities of an electronic records system as being those of "a computer." Such lists should reflect a combination of records management and legal expertise. It is obviously less demanding than either the "*McMullen* standard," or the nine points of proof specified in the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005, section 5.5:[127]

> a) sources of data — what are the sources of the data in the record system;
>
> b) contemporaneous recording — the electronic records are captured and recorded contemporaneously with, or within a reasonable time after, the events to which they relate (but contemporaneous recording within a particular data base is not required);
>
> c) routine business data — the data within a record is of a type regularly supplied to the organization or created by it during its regular activities;
>
> d) data entry — the data base capture and entry procedures are part of the usual and ordinary course of business of the organization and are carried out in accordance with the procedures manual;
>
> e) industry and national standards — the organization conforms to all appropriate standards for records management inputting, importing and storing of data, and for preserving the reliability of data and of the records management system that stores and transmits that data;
>
> f) business reliance — the organization, when making business decisions, relies upon the electronic records in its data bases;
>
> g) software reliability — the software reliably processes the data;
>
> h) recording of system changes — a record of system changes is kept;

---

127 See notes 36, 40, 46 and 50 *supra*, and accompanying text. This standard is summarized in Appendix A.

and,

i) security — security procedures are in place to protect the integrity of the records management system; at least the following should be able to be proved:[128]

1. protection against unauthorized access to data and permanent records;

2. processing verification of data and information in records;

3. safeguarding of communications lines;

4. maintenance of backup copies of records to replace falsified, lost and destroyed permanent or temporary records;

5. retention and disposition of electronic records in compliance with legislated and internal retention periods and disposition

128 As to the security threat to one's data "threatened" by access to the Internet, the following passage is from a decision concerning "defamation on the Internet": *Barrick Gold Corporation v. Lopehandia et al.* (2004), 71 O.R. (3d) 416, [2004] O.J. No. 2329 (Ont. C.A.), per Blair J.A. (Laskin J.A. concurring):

> [30] In the Internet context, these factors must be examined in the light of what one judge has characterized as the "ubiquity, universality and utility" of that medium. In *Dow Jones & Company Inc. v. Gutnick* (10 December 2002), [2002] HCA 56, that same judge — Kirby J., of the High Court of Australia — portrayed the Internet in these terms, at para. 80:
>
> • The Internet is essentially a decentralized, self-maintained telecommunications network. It is made up of inter-linking small networks from all parts of the world. It is ubiquitous, borderless, global and ambient in its nature. Hence the term "cyberspace". This is a word that recognizes that the interrelationships created by the Internet exist outside conventional geographic boundaries and comprise a single interconnected body of data, potentially amounting to a single body of knowledge. The Internet is [page432] accessible in virtually all places on Earth where access can be obtained either by wire connection or by wireless (including satellite) links. Effectively, the only constraint on access to the Internet is possession of the means of securing connection to a telecommunications system and possession of the basic hardware.
>
> [31] Thus, of the criteria mentioned above, the mode and extent of publication is particularly relevant in the Internet context, and must be considered carefully. Communication via the Internet is instantaneous, seamless, interactive, blunt, borderless and far-reaching. It is also impersonal, and the anonymous nature of such communications may itself create a greater risk that the defamatory remarks are believed: see *Vaquero Energy Ltd. v. Weir*, [2004] A.J. No. 84, 2004 ABQB 68, ¶17.

This passage and following, were quoted in, *Beidas v. Picherler* (2008), 294 D.L.R. (4th) 310, [2008] O.J. No. 2135, ¶48 et seq. (Ont. SCJ, Divl. Ct.). And para. 30 was quoted in, *Robertson v. Thomson Corp.* (2004), 72 O.R. (3d) 481, [2004] O.J. No. 4029, ¶30 (Ont. C.A.).

> [disposal] requirements, and documenting such compliance and disposition schedules; and,
>
> 6. a business continuity plan for electronic records and associated data, including off-site copies of essential files, operating and application software [a "disaster recovery" factor].

And, [paraphrasing the next two paragraphs] the use of an electronic record should not violate any legal principles prohibiting the disclosure of privileged or confidential data or information; for example, the principles of the privacy laws. This may be considered a tenth requirement (*i.e.*, insert as "j" above).

These factors should be able to be proved by a single supervising officer, such as the chief records officer of the organization who is accountable for the records systems. An additional witness may be required for software that is unique to the system, unless the supervisor can prove its history of reliability. If not, the programmer who wrote the software should be available to certify its reliability until the software does have a history of reliability. Or, when opposing the admissibility of such records, these factors provide a framework for one's cross-examination. They have the added authority that comes from being within a National Standard of Canada that establishes the basic principles and practices of electronic RM.[129]

At present, that is substantial authority because the case law (other than the "*McMullen* standard"[130]) is unhelpful as to defining the necessary foundation evidence for admissibility under the electronic record provisions. And the subjective nature of the "usual and ordinary course of business" test in the business record provisions means that that test varies with each case and business that adduces records.

The above lists of factors for admissibility can also serve as the foundation for disclosure applications, because the requirements of admissibility should produce the documents with which to test, and if necessary, challenge that admissibility.

The above tests are to be used in satisfaction of three phrases within the *Evidence Act* admissibility requirements for business records:

> (1) "the integrity of the electronic records system,"
>
> (2) "the usual and ordinary course of business;" (or, for the business record hearsay rule exception at common law, "in the routine of business") and,

---

129 It follows that records management policy and procedure should be written to satisfy these factors at any point in the life of a records system, and not only when evidence is needed for legal proceedings or to satisfy any other formal examination or demand in regard to the organization's records and RM system. System corrections made in contemplation of litigation or other formal examination or demand, will undermine the credibility of the records adduced, and of the "systems integrity" sought to be verified and demonstrated. Thus, there are several justifications for the "prime directive" of the national standard, *Electronic Records as Documentary Evidence*, *supra* notes 36, 40, 46, and 50: "an organization shall always be prepared to produce its records as evidence" (at clause 5.4.3 c, p.17 of the standard).

130 *Supra* notes 122–124 and accompanying text.

(3) "the circumstances of the making of the record."

The first phrase is found in the "electronic record" provisions of the Evidence Acts.[131] The second and third are found in the "business record" provisions.[132] All three must be satisfied for records that are (1) recorded or stored in an electronic records system; and, (2) business records.[133] For records that are "relied upon printouts" within the meaning of s. 31.2(2) CEA, s. 34.1(6) OEA, s. 41.4(3) AEA, and s. 23D(2) NSEA, they too will have to satisfy the business record provisions of the Evidence Acts. One might think of these special subsections as providing a fourth key legal phrase.[134]

XI. THE APPROPRIATE ACCOMMODATION OF THE RULES OF EVIDENCE TO ELECTRONIC RM

Six interacting levels of legal and technical evolution in RM perpetuate a corresponding evolution in its rules of evidence.

(a) Evolution of Evidence for Admissibility and "Weight"

Whenever a new technology provides a new type of evidence, or a new procedure for evaluating evidence, there is an initial period of establishing its credibility by expert testimony — a period of establishing the persuasiveness of "novel science." A technician need also be a witness if the expert does not also testify to its application in each case as well as to the validity of the new procedures. *Second*, then follows a period of accepting such evidence by way of a technician who applies it and testifies in each case about the results obtained, without the need for an expert witness. By this stage, an understanding of the technology has become com-

131 For example, s. 31.2 CEA, s. 34.1(5), (5.1) OEA, s. 41.4 AEA, and s. 23D(1) NSEA, or in the Electronic Evidence Acts of Prince Edward Island and Yukon: *Electronic Evidence Act*, R.S.P.E.I. 1988, c. E-4.3, s. 4(1); *Electronic Evidence Act*, R.S.Y. 2002, c. 67, s. 4(1).

132 Section 30 CEA, s. 35 OEA, s. 23 N.S.E.A. Note that "business" includes all types of commercial and institutional activity including that of governments. The AEA does not have a business record provision, making more frequent in Alberta courts the use of the business record hearsay rule exception at common law; (see the references to *Ares v. Venner* (S.C.C., 1970), *supra*, notes 2, 21, 109, 109, and 111, and to the common law *supra* notes 2, 3,23, 93, 111, 113, and 117). But the latter can be used along with an *Evidence Act* business record exception in any jurisdiction where the common law applies. It doesn't have a "notice" requirement as do s. 30(7) CEA and s. 35(3) OEA, nor any "in contemplation of litigation" limitation.

133 For Quebec, instead of these legal phrases being within an *Evidence Act*, comparable provisions can be found in the *Civil Code of Quebec*, S.Q., 1991, c. 64, Articles 2803 to 2874, and in, *An Act to Establish a Legal Framework for Information Technology*, R.S.Q., 2001, c. C-1.1.

134 For analyses of the "relied upon printout provisions," see: Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010) 14 Canadian Criminal Law Review 111 at 150–153; and, Ken Chasse, "Electronic Records as Documentary Evidence," (2007) 6 Canadian Journal of Law and Technology 141 at 152.

mon and accepted. Expert testimony is no longer needed to explain, for example, the difference between electronic records management concepts and paper record concepts. *Third* is the certificate period: a technician sends the results to court by signed certificate. For example, the accused person receives a copy of the certificate containing the breathalyzer readings when the results are obtained and the certificate is signed by the breathalyzer officer. But because of doubts and disturbing results, a less trusting *fourth* period of greater sophistication may intervene, which increases the necessary time for determining admissibility. The above lists of tests mean that the admissibility of electronic records is not purely the product of science and technology. They are not inherently reliable.[135] Nor should courts view electronically produced and stored records as not raising hearsay issues because such statements are not the utterances of humans but of machines and devices. Humans do everything to set electronic devices in motion, including making decisions as to what information will be fed into them, their software and hardware, and their operation and maintenance. Therefore they are no more inherently reliable than humans wish to make them and as reliable as humans make themselves in various situations. Computers are manufactured, tested, and approved only to the point that they are sufficiently reliable to be successful in the marketplace. Beyond that is the area of further profit which is not to be wasted on unmarketable improvements or improvements of only marginal profitability. Electronic records produce hearsay issues.

Therefore the procedures by which the products of science are employed in legal proceedings are constantly changing. As each new technology gains a "track record" of reliability and understanding, admissibility becomes almost routine, then uncontested to save time and costs. Applying it to produce and examine evidence becomes more efficient. Then its presentment as evidence moves from scientists who testify to the validity of its principles, to technicians who apply it, to signed certificates and affidavits without witnesses. In the 1960s, breathalyzer readings were testified to by a police "breathalyzer officer" in every case. *Criminal Code* based certificates came later. Before that, experts had to testify to the validity of the science and mechanisms of breathalyzer machines. Today, no one can meaningfully challenge the principle that no two people have the same fingerprints. But 100 years ago it had to be testified to by a qualified expert in every case. Now we can come no closer to attacking the foundation principles than arguing over how many "points of congruency" are sufficient for a fingerprint identification, or arguing that proper procedures were not used in a particular case. (DNA evidence was at stage one, and now perhaps rushed too soon to "stage three certificate evidence.") Therefore, courts are never justified in refusing to apply new technology because it takes too much court time to accommodate it. That "time" is constantly evolving. And, courts and evidence must reflect and accommodate the working world that produces them. Courts operate on evidence, therefore they cannot shut out the real world until they have time to "catch-up." Therefore, the law of evidence must have

135 Automobiles are also the products of science, whose every automatic operation is now dependent upon electronic devices. Yet, cars are being recalled by their manufacturers in the millions because of serious faults in those devices.

rules for the admissibility and use of "novel science."[136]

(b) Evolution of RM Technology

The records and information produced by electronic technology today did not exist 50 years ago, except for that put out by large institutional mainframe computers. RM now includes *inter alia*, printouts and other renderings from computers of all types, websites, email, text and instant messaging, data from GPS devices, computer animations and simulations, digital photos, the several varieties of imaging, and that of electronic audio and video devices. Most business records were electronically produced before all these varieties of electronic technology existed. Now, it is best to consider all records and information as electronically produced and stored. What historic paper records remain with potentially useful information are quickly being converted to electronic storage then disposed of. There will always be new RM technology going through the various stages of "legal acceptance and accommodation."

George L. Paul states:[137]

> Does each case compel a proponent to prove the reliability of every system, de novo?
>
> No. As many cases recognize, once there is a familiarity with a particular system or process, over time, less and less of a foundational showing is required before evidence is admitted. Do we need litigants proving how a WORD application inserts information as metadata, as a foundation to each and every admission of such metadata? No. But of course, the opponent of the evidence is free to litigate the reliability of the process in question in every case, and to argue the weight of the evidence.
>
> Accordingly, courts should have a broad and powerful discretion about how much to require in each case as a matter of a foundational showing. If a piece of computer-generated information is duplicative, and merely adds to what is already a substantial weight of evidence, and comes from a commonly trusted system, perhaps less of a showing is necessary than when it is practically the only evidence in the case, as occurred with *Vinhnee*.[138]
>
> Further, if the computer-generated information comes from a custom designed, custom-implemented, sparsely distributed or marketed application,

136 *R. c. J. (J.-L.)*, 2000 CarswellQue 2310, 2000 CarswellQue 2311, 2000 SCC 51, [2000] S.C.J. No. 52, [2000] 2 S.C.R. 600 (S.C.C.). As to the safeguards applicable to the use of expert evidence, see: *R. v. Mohan*, 1994 CarswellOnt 1155, 1994 CarswellOnt 66, [1994] S.C.J. No. 36, [1994] 2 S.C.R. 9 (S.C.C.). Those safeguards were most recently reiterated and applied by the Ontario Court of Appeal in, *R. v. Abbey*, 2009 ONCA 624, 2009 CarswellOnt 5008, [2009] O.J. No. 3534, ¶71 to 96 (Ont. C.A.); leave to appeal refused 2010 CarswellOnt 4827, 2010 CarswellOnt 4828 (S.C.C.), under the heading, "The Applicable Principles and a Suggested Approach to Admissibility;" and, *R. v. G. (P.)*, 2009 ONCA 32, 2009 CarswellOnt 123, [2009] O.J. No. 121, 242 C.C.C. (3d) 558, ¶16 to 18 (Ont. C.A.). And in the *Goudge Inquiry Report*, *supra* note 96, at Volume 3, p. 488, there is a list of 14 factors for determining the admissibility of "novel scientific evidence."

137 George L. Paul, *supra* note 13 at 145-46.

138 *In re Vee Vinhnee supra* note 30 and accompanying text.

> or a new application, then a different approach is appropriate than if, for example, a common e-mail system, operating in a common configuration is examined. Courts, in their opinions, generally skip over this important aspect. In some instances, a computer program may only have been written for one or two users. In other instances, many tens of millions of users might use a program daily, and are presumably reporting to publishers about any problems. The foundational determination should take this into account.

This is close to "system discovery," *i.e.*, producing information and documentation as to an electronic records system's state of "system integrity compliance." It is justified by (1) proof of "system integrity" is the test of admissibility; and (2) by the fact that an electronic record is dependent for its integrity and authenticity on its electronic records system. Respectively, it is justified in law and fact.[139]

(c) A Certification Process for "System Integrity"

A "system integrity" test thoroughly applied to both admissibility and disclosure (discovery of documents) would be considerably facilitated by an expert certification of compliance procedure. Specialists in records management, as indepen-

---

139 The failure to make such disclosure of "systems documentation" was successfully argued as a breach of the right to liberty under Charter s. 7 by reason of the absence of "procedural fairness" in relation to a prison transfer from light to medium security in, *May v. Ferndale Institution*, [2005] 3 S.C.R. 809, [2005] S.C.J. No. 84. The Court held (at para. 117) that not only were the factors used in making the transfer decision to be disclosed, but also, "how those values were assigned to them [and] how those values factored into the generation of the final score." That would require disclosure of how the evaluating "SRS" (Security Reclassification Scale) software worked. The appellant was ordered to be transferred back to a minimum security institution. The judgment of LeBel and Fish JJ. for the majority states (at paras. 118–120):

> *118* How can there be a meaningful response to a reclassification decision without information explaining how the security rating is determined? As a matter of logic and common sense, the scoring tabulation and methodology associated with the SRS classification score should have been made available. The importance of making that information available stems from the fact that inmates may [page858] want to rebut the evidence relied upon for the calculation of the SRS score and security classification. This information may be critical in circumstances where a security classification depends on the weight attributed to one specific factor.
>
> *119* Hence, given the importance of the information contained in the scoring matrix, the presumptive validity of the score and its potential effect on the determination of security classification, it should have been disclosed. The respondents had a duty to do so under s. 27(1) of the *CCRA*. [the *Corrections and Conditional Release Act*, S.C. 1992, c. 20]
>
> *120* In conclusion, the respondents failed to disclose all the relevant information or a summary of the information used in making the transfer decisions despite several requests by the appellants. The respondents concealed crucial information. In doing so, they violated their statutory duty. The transfer decisions were made improperly and, therefore, they are null and void for want of jurisdiction. It follows that the appellants were unlawfully deprived of their liberty.

dent experts, would examine and certify compliance of electronic record systems with the National Standards of records management. That is one of the intended purposes of the "use of standards" provisions such as s. 31.5 CEA, s. 34.1(8) OEA, s. 41.6 AEA, and s. 23F NSEA. Such certification of large electronic record systems is growing and will become common, then routine. The need for "legal compliance" grows with every new statute dependent upon good records management. Then, it will become required records management practice. For smaller systems, "system integrity" will be easily proved — the records manager can testify to, or by affidavit warrant compliance with the National Standards of Canada[140] (a procedure not unlike an affidavit under the banking record provisions such as s. 29 CEA).[141] Such affidavits are provided for in the electronic record provisions.[142] Thus the application of laws that make use of electronic records, and laws dependent upon good electronic RM will evolve as RM electronic technology evolves and a common need for "system integrity" grows. There are certification processes underlying many types of evidence now — from expert witnesses (the "qualifications" voir dire is a certification process) to breathalyzer machines,[143] and the certification process imposed by s. 5 of PIPEDA[144] upon private organizations to comply with the National Standard of Canada, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96,[145] or a provincial counterpart if there is one.[146] Certification cuts down the evidence and time needed for obtaining and determining admissibility, and limits the opposition to admissibility.[147] And, it will

140 *Supra* notes 40 and 53 and accompanying text.

141 Because banking records are so frequently made evidence, and seldom is the bank involved as a party to such proceedings, s. 29 CEA allows bank personnel to warrant by affidavit (s. 29(2)) that the records satisfy the s. 29 requirements as to "true copies" of the bank's records "made in the usual and ordinary course of business," *etc.* Thus bank personnel don't have to be attending witnesses in such proceedings. Similar provisions exist in the provincial and territorial "banking record" provisions.

142 For example in, *e.g.*, s. 31.6 CEA, s. 34.1(9) OEA, s. 41.7 AEA, and, s. 23G NSEA.

143 See *Criminal Code* s. 258, and the resulting "Approved Breath Analysis Instruments Order" Regulations, *supra* note 33.

144 PIPEDA, *supra* notes 33, 46, and 52.

145 *Supra* notes 34 and 52.

146 Only three provinces have enacted laws comparable to the "Protection of Personal Information" requirements of Part 1 of PIPEDA (*supra* notes 33, 46, and 52) British Columbia, Alberta, and Quebec. The other provinces are required to comply until they do enact such legislation; see the Regulation making powers in s. 26(2)(b) to so exempt provinces.

147 The device, procedure, or standard that is used to create and certify the evidence, being statutorily designated and approved, its appropriateness and competence cannot be attacked, except by attacking the statutory approval process itself by way of a superior or conflicting enactment, *e.g.*, constitutional rights to "fair trial," "fundamental justice," and "full answer and defence" (Charter, *supra* note 106, ss. 7 and 11(d)), or the "full answer and defence" provisions of the *Criminal Code* itself, ss. 276(3)(a), 650(3), and 802(1)). For an analysis of these arguments see the article, Ken Chasse, "Electronic Discovery in the Criminal Court Process," (2010), 14 Canadian Criminal Law Review 111.

reduce the time needed for and complexity of discovery and the motions and other court proceedings resulting from it.[148]

(d) Record Formats have Different Rules of Admissibility

Most RM systems have records in several formats, from records on paper, to records on microfilm and in electronic format. Various divisions of an organization could have some or all five of the following types of records — each having different legal rules for determining its admissibility and "weight" (probative value, credibility) as evidence:

1. original paper records;[149]
2. electronic records, *i.e.*, they are created or stored electronically;[150]
3. microfilmed or imaged records;[151]
4. "relied upon printouts" of electronic records within the meaning of s. 23D(2) NSEA, s. 31.2(2) CEA, s. 34.1(6) OEA, and s. 41.4(3) AEA;[152]
5. records created through EDI (electronic data interchange) for which the advantages of s. 31.5 CEA, s. 34.1(8) OEA, and s. 41.6 AEA are

148 The Canadian General Standards Board, the author and sponsoring agency of The National Standards of Canada, *supra* notes 41 and 42, has been asked by those in the records management and legal professions to create a certification process and train records management specialists who can certify electronic records systems as being in compliance with its national standards. The need for a certification system and comparisons with existing certification systems are more fully developed in the article, Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111 beginning at 153.

149 Admissible as business records under s. 30 CEA, s. 35 OEA, and s. 23 NSEA, and by way of the business record exception at common law, *supra* notes 78 and 80, and *Ares v. Venner* (S.C.C., 1970) *supra* notes 2, 21, 109, 111 131, and its progeny (case law).

150 The electronic record provisions are: ss. 31.1 to 31.8 CEA; s. 34.1 OEA, ss. 41.1 to 41.8 AEA, and, ss. 23A to 23H NSEA. Electronic business records will also have to satisfy the business record provisions, *ibid*.

151 Admissible under the microfilm provisions (s. 31 CEA, s. 40 AEA, s. 22 NSEA, and s. 34 OEA), or the electronic record provisions, *ibid.*, as in the case of COM, computer output microfilm.

152 "Relied upon printouts": Admissible because they are, "manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout," *i.e.*, admissible independent of their electronic origin and therefore of the "system integrity" (good or bad state) of the electronic record system in which they were originally recorded or stored. (Whether these special provisions will be given that interpretation is yet to be seen.) Therefore compliance with the national electronic RM standards would be inapplicable if "relied-upon printouts" are considered to be paper-original documents and not electronically-produced records. An example of such a printout would be a contract or other official document whose interpretation, contestation, or other use would be based entirely upon its paper form, its electronic origins having no part in any such interpretation or dispute.

available.[153]

Records managers have to be instructed accordingly if they are to give adequate "foundation evidence" for admissibility.

(e) The Transition from RM as Good Business Practice to RM for "Legal Compliance."

Since 2000, major laws have been enacted that depend upon high quality electronic RM — being laws, without precedent in Canada, as to[154] (1) electronic records provisions in the Evidence Acts; (2) electronic commerce; (3) personal information protection and privacy; (4) electronic discovery; (5) RM National Standards of Canada; and, (6) the records and information management requirements of government departments and agencies, *e.g.*, those of taxing departments[155] and securities commissions.[156] These, without more, constitute a regime of "legal compliance" imposed upon on all electronic RM. It is no longer merely good business practice to conduct RM according to recognized standards. It is a matter of law — laws comprised of these six subjects (in addition to laws on specialized subjects).

And such "legal compliance" will include laws as to electronic signatures; the regulation of all major industries, professions, and services; and personal identification. Electronic technology greatly magnifies the need to use hearsay evidence in proof of communications and transactions because it removes the need for face-to-face communications and transactions. It greatly reduces the need for witnesses "having direct personal knowledge" of such events by correspondingly enabling the use of records as evidence. That in turn requires the standardization and enforcement of RM principles and practices. That fact means that every new law extending the use of electronic technology will have to extend the area of legal compliance as to RM.

(f) Admissibility Acquires, Then Requires Canada's National Standards of RM

Changing forensic attitudes towards the efficacy of various developments in science and technology and the evidence it produces determine the appropriate rules of evidence to be applied and how to apply them. Not the converse. Those attitudes are most quickly changed by changes in expert knowledge and expert tes-

---

153 Section 31.5 CEA, s. 34.1(8) OEA, s. 23F NSEA, and s. 41.6 AEA have two purposes: (1) to put beyond doubt that standards, particularly RM standards, may be used in determining the admissibility of electronic records, "under any rule of law"; and, (2) to facilitate the use of trading partner agreements, "on how electronic records are to be recorded or stored." This second usage gives legal recognition to privately contracted protocols containing rules of evidence applicable to a high volume flow of electronic records between two individuals or institutions, *e.g.*, EDI, as between a manufacturer and its parts suppliers, or a government and its government-supported agencies by way of computer-to-computer orders and agreements.

154 See also notes, 18 to 21, 29, and accompanying texts *supra*.

155 See for example the Canada Revenue Agency's requirements in note 46 *supra*.

156 See for example the Ontario Securities Commission's requirements in note 27 *supra*.

timony. The National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 can be used as very effective expert knowledge and testimony as to the requirements of electronic records and information management.[157] If used as intended, the requirements for admissibility will evolve compatibly with the principles and practice of electronic RM.

I say this as much because of the case law and legislative history of laws concerning the admissibility of records as evidence, as for the need for an authoritative standard that makes RM law and practice compatible. Issues concerning such provisions don't get decided often enough nor quickly enough, and the legislative drafting mentality still is (1) "if it ain't broke, don't fix it"; and, (2) "be vague because black-letter, well defined and exclusive, legislated definitions as to 'foundation evidence for admissibility' could exclude good records and records systems; so let the judges decide what's right for each case." Therefore amendments don't happen until a court decision causes a crisis as happened when *Myers v. D.P.P.* (H.L., 1965),[158] caused business record hearsay exceptions to be added to Canada's Evidence Acts. Those provisions have been in the Evidence Acts since the late 1960s, but their major defects are still the stuff of law journal and textbook literature because they have not been remedied by amendment or case law. And the electronic records provisions have been in the Evidence Acts since 2000, but there are still no decisions providing analysis of their key phrases such as the "system integrity test." And they were enacted more than 40 years after the business record provisions were enacted, and at least 40 years after electronic technology showed that it would soon dominate the production of business records.[159] Why? Because that which doesn't need to be decided, doesn't get decided, nor fixed. Lawyers consent to the admissibility of each other's records (to save time and costs), so issues don't get raised and decided. And very few lawyers know enough about RM principles and practices to mount effective challenges to the admissibility and "weight" of records. Those challenges they perceive to require expensive expert investigation, advice, and testimony that the client, Legal Aid, public defender, or

---

157 The other RM National Standard of Canada, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB 72.11-93, *supra* notes 40 and 41 and accompanying text, is still the "industry standard" in regard to imaging. But its "legal sections" should not be relied upon because they were written before the electronic record provisions of the Evidence Acts were enacted.

158 *Supra* note 2.

159 *Supra* note 79. The Minister of Justice and Attorney General of Canada, John Turner, told the House of Commons on January 20, 1969, (Hansard, Commons Debates, p. 4496), "It is therefore apparent that the law in this country has fallen far behind the major changes which the computer age has brought to business methods." As a result, a bias toward a "low threshold of admissibility" was confirmed on that occasion by his statement, "I consider that, in general, the law of evidence should be moving away from the rigid rules of admissibility toward assessment of the cogency of logically relevant facts. If the facts are relevant, what is the best way to introduce those facts without there being any unfairness to either side? Accordingly, Mr. Speaker, this bill would, subject to certain safeguards, render business records as defined in the bill generally admissible and would entrust the courts with the discretion of assessing the probative value of those documents."

legal services clinic won't pay for. Therefore the legislative drafting mentality aggravates the shortcoming that is this absence of case law.[160]

But how and what to prepare for trial in regard to records as evidence? And what to tell a RM manager asking if major electronic technology alterations to his/her records system will affect the use of records in court, or in regard to the "legal compliance" régime discussed above?[161] Therefore, the National Standard of Canada, *Electronic Records as Documentary Evidence*,[162] can provide an ongoing, updateable standard by which to develop the necessary rule of admissibility for electronic records in a principled way.[163] The records manager is to be told that alterations "in contemplation of litigation" raise an inference as to the absence of "system integrity"; and, (2) the "Prime Directive," an organization shall always be prepared to produce its records as evidence."[164] Such state of readiness is necessary for (1) ascertaining efficiently and accurately what records are available to be used as evidence or disclosed for "document discovery"; (2) making discovery and disclosure of records; and, (3) making "RM systems" discovery, *i.e.*, information and documentation as to the system's state of compliance with the "system integrity" standard as measured by the National Standard, which should also be required as foundation evidence for arguments as to admissibility.

XII. SUMMARY OF CONCEPTS, PRINCIPLES, AND POINTS MADE

1. Paper record systems are based on "records" concepts; electronic record systems are based on "systems" concepts. The business record provisions of the Evidence Acts, including U.S. Federal Rule of Evidence 803(6), were enacted when "records" concepts were the conceptual basis of legislation in regard to the use of records as evidence.

---

160 These "realities" have to be taken into account when legislating, particularly in adopting and adapting legislation from other countries.

161 See the previous section.

162 *Supra* notes 40 and 53.

163 The section in the electronic records provisions that refers to the use of standards doesn't cite *the standard*, but its express linking of such standards as an aid in deciding issues of admissibility provides the necessary involvement of the law with in RM. It allows a flexible, adaptable test of admissibility to be authoritatively supplemented so that there is sufficient certainty for: (1) preparation for trial; (2) conducting an examination-in-chief and cross-examination; and, (3) for advising RM technicians and managers responsible for large and small electronic records systems (see: s. 31.5 CEA; s. 23F NSEA; s. 34.1(8) OEA; and, s. 41.6 AEA). In addition, the Canada Revenue Agency has added references to *the standard* in its Information Circulars concerning records requirements for taxpayer records (*supra* note 46). Now, many large private and public sector institutions are having their electronic records systems and "systems alterations" expertly evaluated as to compliance with this National Standard of Canada. For a discussion of these issues concerning the interdependence of RM law and RM practice, see: Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111 at 123–157.

164 *Supra* note 41 and accompanying text.

2. "Records" concepts judge a record by its own history, as do the business record provisions; "systems" concepts judge a record by the electronic records system in which it is recorded or stored.

3. The business record provisions contain a "business activity" wording for their rule of admissibility. Therefore they are "subjective" in that the creation and use of records within the usual business activity of the organization from which the records come is the requirement for admissibility. In contrast, the electronic record provisions are "objective" in that proof of the "system integrity" of the electronic records system from which the records come is the requirement for admissibility under their unique version of the best evidence rule. The business record provisions deal with hearsay issues; the electronic record provisions deal with best evidence rule issues. An electronic business record must satisfy both sets of provisions if both a hearsay and a best evidence rule issue are raised.

4. All provinces, territories, and the federal jurisdiction in Canada have enacted electronic record provisions except the two provinces of British Columbia and Newfoundland and Labrador.

5. The B.C. *Evidence Act* contains a business record provision but not an electronic record provision. Therefore both hearsay and best evidence rule issues in regard to an electronic business record would be dealt with under that provision.

6. The *Evidence Act* in Newfoundland and Labrador contains neither a business record nor an electronic record provision. Therefore both hearsay and best evidence rule issues would be dealt with under the common law rules.

7. The authentication rule in Canada in regard to records states simply: "The person seeking to introduce an electronic record has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be." The American authentication rule is broader in that it requires proof that the record contains authentic evidence of what it purports to prove. It thus provides an initial assessment of the reliability of the record. Therefore, it appears to deal, in a preliminary fashion, with what would be left to the hearsay rule in Canada.

8. However, U.S. FRE 803(6) contains a business record hearsay exception requiring proof that the record etc., was, "kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation." The Canadian business record hearsay exception in the Evidence Acts uses comparable "business activity" wordings such as, "made in the usual and ordinary course of business."

9. Such admissibility rules are no longer able to provide adequate protection against the use of unreliable records as evidence. The "business activity" admissibility rule is no longer adequate because profit is no longer the only motivation controlling records management. Their shortcomings and unanswered issues are set out above. Therefore the "system integrity" test is necessary.

10. These business record provisions also contain wordings that direct attention to the "circumstances of the making of the record." Section 30(6) of the *Canada Evidence Act* may therefore be the predominant test of admissibility in s. 30 in that if such "circumstances" are deemed inadequate, the record could be ruled inadmissible. Therefore s. 30(6) is an exclusionary rule. The comparable words in FRE 803(6) serve the same purpose: ". . . unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness." In con-

trast, the comparable subsections in the other Evidence Acts in Canada are limited in application to "weight." If all such "circumstances of the making" provisions applied to admissibility as well as to weight, they could be interpreted to require proof of "system integrity" comparable to that required by the electronic record provisions.

11. The comparable "business activity" phrase in the common law business record exception is, "in the routine of business." The common law rule in Canada was revised by the Supreme Court of Canada in, *Ares v. Venner*, [1970] S.C.R. 608, 12 C.R.N.S. 349, 14 D.L.R. (3d) 4, approximately one year after s. 30 was added to the *Canada Evidence Act*. Similar provisions were added to the other Evidence Acts in the late 1960s, except for the *Evidence Act* of Alberta and Newfoundland and Labrador. Therefore they still use the common law rule. However, the common law rule can be used together with a statutory provision.

12. The National Standards of Canada concerning records management can provide the necessary detailed content of the "system integrity" test of admissibility in the electronic record provisions. They are: *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005; and, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93. The electronic record provisions make such standards relevant "under any rule of law" in determining the admissibility of an electronic record. Therefore these standards can be used when applying the "circumstances of the making of the record" provisions in the business record sections of the Evidence Acts to electronic records.

13. Serious, common defects in electronic RM practices are referred to because the admissibility and "weight" of electronic business records should be interdisciplinary determinations — law and record management principles.

14. Admissibility and electronic discovery are very interdependent. Both require "RM systems discovery" and not just the disclosure and production of relevant records. The integrity of electronic records is dependant upon "the integrity of the electronic records system in which they are recorded or stored," Therefore "system discovery" is required in relation to both discovery and admissibility, and thereafter for determinations of "weight" (probative value and trustworthiness).

15. Because there are now many Acts dependent upon and demanding good records management practice and the production of records, records management is now controlled by the principle of "legal compliance" and not just by good business practice.

16. The different records formats have different rules of admissibility. Paper, electronic, and microfilm records, "relied-upon printouts" and records created through electronic data interchange (EDI), all have their own admissibility rule.

17. The best evidence rule should be abolished. Its use in the electronic record provisions as the basis for the "system integrity" test is a contradiction of the traditional rule in several respects. If the business record provisions are to be kept (which is not necessary), the electronic record provisions should be redrafted as "authentication" provisions using the American concept of the authentication rule.

18. A single section for the admissibility of all business records, based upon the "system integrity" concept, should replace the current three phrases in the business and electronic record provisions in the Evidence Acts: (1) "the integrity of the electronic records system"; (2) "the usual and ordinary course of business"; and, (3) "the circumstances of the making of the record."

19. The electronic record provisions have brought several improvements. Particularly important are: (a) giving electronic records a legal status equal to that of "paper original" records, thus enabling the destruction of paper records once they have been placed into secure electronic records management environment; and (b) expressly made relevant the use of national and international records management standards in relation to determinations of the admissibility and "weight" of electronic records. The National Standards of Canada are particularly useful for this purpose.

20. To facilitate admissibility and electronic discovery, an authoritative certification process for electronic records systems as being compliant with the requirements of the National Standards of Canada should be established by the Canadian General Standards Board, the sponsor of those standards.

Appendix A — Summary of RM system compliance standards established by the National Standard of Canada, Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005 ("72.34")[165]

The principal groupings of the principles provided by *72.34* are: [The square bracketed references that follow each, refer to sections and paragraphs within the national standard, *72.34*.]

> 1. Management authorization and accountability: to test that records and document management receives authoritative recognition from senior management. [5.4.3] This is an essential aspect of a RM (records management) system's "system integrity," and "usual and ordinary course of business," which are requirements of the Evidence Acts.
>
> 2. Documentation: to test whether sufficiently detailed and unambiguous documentation exists for the procedures used to manage records and documents; that this documentation is sufficiently known to all parties that have access to modify the electronic records in any manner; and that the guidance in this documentation is followed by all such parties at all times.
>
> 3. Reliability: Reliability of electronic records is tested according to the following legal rules:
>
> > Authenticity: to test whether records and documents actually come *only* from the person, organization or other legal entity asserting to be their author or authorizing authority. [5.2.2]
> >
> > Integrity: the electronic records provisions of the Evidence Acts state that where any such record is challenged as to whether it is a reliable copy of its electronic source, such challenge is satisfied by, "evidence of the integrity of its electronic

165 Only *72.34* is summarized, because it is comprehensive of all electronic records, including those of the other National Standard of Canada *72.11*, *Microfilm and Electronic Images as Documentary Evidence*. However, *72.11* is still the "industry standard" for the RM requirements of imaging.

> records system by or in which the data was recorded or stored." Therefore, proof of the integrity of any particular electronic record is established by proof of the integrity of the electronic RM system that recorded or stored it — this is the "system integrity test" of admissibility for electronic records (the acceptability of records in legal proceedings). [5.2.3] To aid proof of such "system integrity," the electronic records provisions of the Evidence Acts provide three presumptions that are paraphrased in subsections of the national standard [5.2.3(a), (b), (c)].

4. The procedures manual and chief records officer: to test whether there is a current manual covering all policies, procedures, and systems in regard to all records and information management. Again, authorization, accountability, and documentation for such a manual, and for the creation of the position of chief records officer should be based upon a bylaw, or order of similar authority within the organization. There can be one or more manuals covering these functions. [5.4.2; 5.4.3]

5. Readiness to produce (the "Prime Directive"). *"An organization shall always be ready to produce its records as evidence."* [5.4.3c, at p. 17] Measuring the readiness to produce its records by gauging the organization's ability to produce an human-readable or human-viewable version of any document or record. "This dominant principle applies to all of the organization's business records including electronic, optical, original paper source records, microfilm and other records of equivalent form and content." [5.4.3c; 5.4.1c]

6. The "usual and ordinary course of business," and "system integrity": to test whether: (1) the electronic documents or records that are to be used as documentary evidence have been recorded, stored, and used in the organization's usual and ordinary course of business, *i.e.*, within its normal, approved practices and procedures; and, (2) the "system integrity" of the RM system those records come from. [5.2.1b, c] These tests from the Evidence Acts refer to the organization's records and information management, and not simply the usual and ordinary course of business of its chief records officer. It is what senior management has approved by bylaw (or order of comparable authority), not what its chief records officer has invented or improvised. Such is an important factor in proof of "system integrity." [6.2.1; 6.2.2]

7. Retention and Disposal: to test that an appropriate retention program has been documented and is followed. RM policy should provide guidelines for records storage, protection, and retention so that records remain available and usable as required for decision-making, program-service delivery, and accountability. Disposal should occur in accordance after business, legal, and audit requirements have been served and the applicable retention periods have expired, such disposal being formally documented. [6.8; 6.9]

8. Backup and system recovery: to test whether appropriate backup procedures are in place and maintained. [6.10]

9. Security and protection: to test whether appropriate security is in place

and is maintained. [6.12]

10. Quality Assurance Program: to test whether a quality assurance program is in place and is adequate, including periodic confirmation reviews conducted by independent audit to verify compliance. [7]

11. Audit Trail: to test whether audit trails are in place and are adequate to provide evidence of the authenticity of stored records. [8]

12. Additional tests that touch on related areas such as system management, workflow, and version control. [8; Annexes A, and C]

There are more than 200 specific compliance tests that are applied to determine if the individual principles are being complied with. The analysts — a combined team of records management and legal expertise — analyze: (1) the nature of the business involved; (2) the uses and value of its records for its various functions; (3) the likelihood and risk of the various types of its records being the subject of legal proceedings, or of their being challenged by some regulating authority; and, (4) the consequences of the unavailability of acceptable records — for example, the consequences of its records not being accepted in legal proceedings. It follows that the details of good electronic RM practice may differ substantially from one organization to another. And, to determine adherence to the above tests, an examination of the RM of every department would have to be conducted. For example, a government auditor may require that such an independent assessment of the RM of a government agency, board, or commission, or of a university records system be conducted. And for business organizations as well, the consequences of failing to comply are equally applicable and threatening to their viability.

Similarly, in regard to the older national standard, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93, there is a comparable series of more than 50 tests that are applied to determine the state of compliance with its principles.

Appendix B — A List of Electronic Commerce Acts and Electronic Record and Business Record Provisions in the Evidence Acts in Canada

Canada (Federal)

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Parts 2 and 3,
Canada Evidence Act, R.S.C. 1985, c. C-5, ss. 31.1 to 31.8, 30.

Alberta (no business record provision)

Electronic Transactions Act, R.S.A. 2000, c. E-5.5,
Alberta Evidence Act, R.S.A. 2000, c. A-18, ss. 41.1 to 41.8.

British Columbia (no electronic records provision)

Electronic Transactions Act, S.B.C. 2001, c. 10,
Evidence Act, R.S.B.C. 1996, c. 124, s. 42.

Manitoba

The Electronic Commerce and Information Act, C.C.S.M. c. E55,
The Manitoba Evidence Act, C.C.S.M. c. E150, ss. 51.1 to 51.8, 50 49.

New Brunswick

Electronic Transactions Act, S.N.B. 2001, c. E-5.5,
Evidence Act, R.S.N.B. 1973, c.E-11, ss. 47.1, 47-2, 49.

Newfoundland and Labrador

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

Nova Scotia

Electronic Commerce Act, S.N.S. 2000, c. 26,
Evidence Act, R.S.N.S. 1989, c. 154, ss. 23A to 23G, 23.

Ontario

Electronic Commerce Act, 2000, S.O. 2000, c. 17,
Evidence Act, R.S.O. 1990, c. E.23, s. 34.1, 35.

Prince Edward Island

Electronic Commerce Act, R.S.P.E.I. 1988, c. E-4.1,
Electronic Evidence Act, R.S.P.E.I. 1988, c. E-4.3.
Evidence Act, R.S.P.E.I. 1988, c. E.11, s. 32.

Quebec

An Act to Establish a Legal Framework for Information Technology, R.S.Q. 2001, c. C1-1,
Civil Code of Quebec, S.Q. 1991, c. 64, Articles. 2803 to 2874.

Saskatchewan

The Electronic Information and Documents Act 2000, s.s. 2000, c. E7.22,
The Evidence Act, S.S. 2006, c. E-11.2, ss. 54 to 59.

Yukon

Electronic Commerce Act, S.Y. 2000, c. 10,
Electronic Evidence Act, S.Y. 2000, c. 11.
Evidence Act, R.S.Y. 2002, c. 78, s. 49.
Evidence Act, R.S.Y. 2002, c. 78, s. 39.

Northwest Territories (no electronic commerce Act)

Evidence Act, R.S.N.W.T. 1988. c. E-8, s. 37.1, s. 47.

Nunavut

Electronic Commerce Act, S. Nu. 2004, c. 2004, c. 7,
Evidence Act, R.S.N.W.T. (Nu.) 1988. c. E-8, s. 37.1.

Appendix C — Legislation Grid — Electronic Record Provisions — Alberta, Canada, Ontario, & Nova Scotia Evidence Acts Incorporate the *Uniform Electronic Evidence Act*

Ken Chasse, Barrister and Solicitor, Toronto, kchasse@fixy.org

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
Note: the UEEA, being the source of this legislation is below at pp. 71-72.	amended by adding s. 33 of the, *Electronic Transactions Act*, S.A. 2001, c. E-6.5 http://www.qp.gov.ab.ca/documents/acts/E05P5.cfm	Federal Bill C-6, ss.56 & 57 *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5, Part 3 In force May 1, 2000	Ontario Bill 11, S.O. 1999, c.12, Sch. B, s.7 In force, June 30, 2000, and later amended by, S.O. 2000, c. 26, Sch. A. s.7 re sub-ss. 34.1(5), (5.1), In force, April 14, 2001	
Section of the amending Act	s. 33 of *Electronic Transactions Act*, added the following sections to the Alberta *Evidence Act*	s. 56 of Part 3 adds the following sections to the Canada *Evidence Act*	s. 7(2) of Bill 11 added the following section to the *Evidence Act* of Ontario:	
Definitions	41.1 In this section and sections 41.2 to 41.8, (a) "electronic record" means information that	31.8 The definitions in this section apply in sections 31.1 to 31.6. "computer system" means a device that, or a group of interconnected or related devices one or more of which,	34.1(1) In this section, — "data" means representations, in any form, of information or concepts: ("données)	23A In this Section and Sections 23B to 23H, (a) "data" means representations, in any form, of information or concepts;

Legal Issue	Alberta Evidence Act R.S.A. 2000, c. A-18	Canada Evidence Act R.S.C. 1985, c. C-5	Evidence Act (Ontario) R.S.O. 1990, c. E.23	Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.
	(i) is recorded or stored on any medium in or by a computer system or other similar device, and (ii) can be read or perceived by a person or a computer system or other similar device, and includes a display, printout or other output of that information, other than a printout referred to in section 41.4(3); (b) "electronic records system" includes the computer system or other	(a) contains computer programs or other data; and (b) pursuant to computer programs, performs logic and control, and may perform any other function. "data" means representations of information or of concepts, in any form. "electronic document" means data that is recorded or stored on any medium in or by a computer system or	— "electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device, and includes a display, printout or other output of that data, other than a printout referred to in subsection (6); ("document électronique")	(b) "electronic record" 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 and includes a display, printout or other output of that data, other than a printout referred to in subsection 23D(2); (c) "electronic records system" includes the computer system or other

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
	similar device by or in which information is recorded or stored, and any procedures related to the recording and storage of electronic records.	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. "electronic 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.	— "electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records. ("système d'archivage électronique")	similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
Application and power of court	41.2(1) Sections 41.3 to 41.8 do not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.	"secure electronic signature" means a secure electronic signature as defined in subsection 31(1) of the *Personal Information Protection and Electronic Documents Act*.	34.1(2) This section does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.	23B (1) Sections 23C to 23H do not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.
	(2) A court may have regard to evidence adduced under sections 41.3 to 41.8 in applying any common law or statutory rule relating to the admissibility of records.	31.7 Sections 31.1 to 31.4 do not affect any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence.	34.1(3) A court may have regard to evidence adduced under this section in applying any common law or statutory rule relating to the admissibility of records.	(2) A court may have regard to evidence adduced under Sections 23C to 23H in applying any common law or statutory rule relating to the admissibility of records. *2002, c. 17, s. 2.*

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
Authentication Rule Establishing "Authenticity"	41.3 A person seeking to introduce an electronic record as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.	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.	34.1(4) The person seeking to introduce an electronic record has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.	23C The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.
Best Ev. Rule Application, and the "relied upon printout"	41.4(1) Subject to subsection (3), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system.	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	s.34.1(5) Subject to subsection (6), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic record.	23D (1) In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

Legal Issue	Alberta Evidence Act R.S.A. 2000, c. A-18	Canada Evidence Act R.S.C. 1985, c. C-5	Evidence Act (Ontario) R.S.O. 1990, c. E.23	Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.
	(2) The integrity of an electronic record may be proved by evidence of the integrity of the electronic records system by or in which the information was recorded or stored, or by evidence that reliable encryption techniques were used to support the integrity of the electronic record.	(b) if an evidentiary presumption established under section 31.4 applies. (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.	s.34.1(5.1) The integrity of the electronic record may be proved by evidence of the integrity of the electronic records system by or in which the data was recorded or stored, or by evidence that reliable encryption techniques were used to support the integrity of the electronic record.	(2) In any legal proceeding, an electronic record in the form of a print-out that has been manifestly or consistently acted on, relied upon or used as the record of the information recorded or stored on the printout is the record for the purposes of the best evidence rule.

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
	(3) An electronic record in the form of a printout that has been manifestly or consistently acted on, relied on or used as the record of the information recorded or stored on the printout is the record for the purposes of the best evidence rule.		s.34.1(6) An electronic record in the form of a printout that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, is the record for the purposes of the best evidence rule.	
Presumption of Integrity	41.5 For the purposes of section 41.4(1), in the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is proved	31.3 For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven	s.34.1(7) In the absence of evidence to the contrary, the integrity of the electronic records system by or in which an electronic record is recorded or stored is proved for the purposes of subsection (5),	23E In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding

Legal Issue	Alberta Evidence Act R.S.A. 2000, c. A-18	Canada Evidence Act R.S.C. 1985, c. C-5	Evidence Act (Ontario) R.S.O. 1990, c. E.23	Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.
	(a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system,	(a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;	(a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;.	(a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;
	(b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it, or	(b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or	b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or	(b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
	(c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce it.	(c) if it is established that the electronic document 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.	(c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceeding and who did not record or store it under the control of the party seeking to introduce the record.	(c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
Standards as evidence — national, international (ISO), and industry standards, and procedures and practices	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.	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.	s.34.1(8) 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.	23F For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in any legal proceeding 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.

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
Affidavits — Proof by — Cross-examination	41.7 The matters referred to in sections 41.4(3), 41.5 and 41.6 may be established by an affidavit given to the best of the deponent's knowledge or belief.	31.6 (1) The matters referred to in subsection 31.2(2) and sections 31.3 and 31.5 and in regulations made under section 31.4 may be established by affidavit.	s.34.1(9) The matters referred to in subsections (6), (7) and (8) may be established by an affidavit given to the best of the deponent's knowledge and belief.	23G The matters referred to in subsection 23D(2) and Sections 23E and 23F may be established by an affidavit given to the best of the deponent's knowledge or belief. *2002, c. 17, s. 2.*
	41.8(1) A deponent of an affidavit referred to in section 41.7 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who affidavit or caused the affidavit to be introduced.	(2) A party may cross-examine a deponent of an affidavit referred to in subsection (1) that has been introduced in evidence (a) as of right, if the deponent is an adverse party or is under the control of an adverse party; and	s.34.1(10) A deponent of an affidavit referred to in subsection (9) that has been introduced in evidence may be cross-examined as of right by a party to the proceeding who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.	23H (1) A deponent of an affidavit referred to in Section 23G that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

Legal Issue	**Alberta Evidence Act R.S.A. 2000, c. A-18**	**Canada Evidence Act R.S.C. 1985, c. C-5**	**Evidence Act (Ontario) R.S.O. 1990, c. E.23**	**Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.**
	(2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in section 41.5(c).	(b) with leave of the court, in the case of any other deponent.	s.34.1(11) Any party to the proceeding may, with leave of the court, cross-examine a person referred to in clause (7)(c).	(2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in clause. 23E(c).
Repeal (abolish) Retention periods re microfilming	[No provision to be repealed in the *Alberta Evidence Act*]	[No provision to be repealed in the *Canada Evidence Act*]	s. 7(1) Subsections 34(3) and (4) of the *Evidence Act* are repealed.	[No provision to be repealed in the Nova Scotia *Evidence Act*]
Canada Gazette as proof of official documents	—	s.57 Subsection 32(2) of the Act is replaced by the following:	[The *Evidence Act* of Ontario contains the following provision:]	—

Legal Issue	Alberta Evidence Act R.S.A. 2000, c. A-18	Canada Evidence Act R.S.C. 1985, c. C-5	Evidence Act (Ontario) R.S.O. 1990, c. E.23	Evidence Act (N.S.) R.S.N.S. 1989, c. 154 S.N.S. 2002, c. 17, s. 2.
		32(2) All copies of official and other notices, advertisements and documents published in the *Canada Gazette* are admissible in evidence as proof, in the absence of evidence to the contrary, of the originals and of their contents.	s.28. Copies of proclamations and of official and other documents, notices and advertisements printed in the *Canada Gazette*, or in *The Ontario Gazette*, or in the official gazette of any province or territory in Canada are *prima facie* evidence of the originals and of the contents thereof.	

Appendix D

Uniform Electronic Evidence Act (UEEA) **As adopted by the Uniform Law Conference of Canada in 1998. The UEEA with commentary at: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2**
Sec 1: Definitions In this Act, (a) "Data" means representations in any form, of information or concepts; (b) "Electronic Record" means data that is recorded or stored on any medium or by a computer system or similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other of output of that data, other than a printout referred to in Subsec 4(2); (c) "Electronic Records System" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.

Uniform Electronic Evidence Act (UEEA) **As adopted by the Uniform Law Conference of Canada in 1998. The UEEA with commentary at: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2**
Application and power of court 2.(1) This Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence. 2.(2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.
Authentication Rule — establishing "authenticity" 3. The person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.
Best Evidence Rule and "relied upon printouts" 4.(1) [In any legal proceeding,] subject to Subsection 2, where the best evidence rule is applicable to an electronic record, that rule is satisfied in respect of the electronic record on proof of the integrity of the electronic records system in or by which the data was recorded or stored. 4.(2) [In any legal proceeding,] An electronic record in the form of a print-out that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the print-out, is the record for the purpose of the best evidence rule.
Presumption of Integrity 5. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding] (a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record; and there are no other reasonable grounds to doubt the integrity of the electronic records system; (b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or (c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Uniform Electronic Evidence Act (UEEA) **As adopted by the Uniform Law Conference of Canada in 1998. The UEEA with commentary at: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2**
Standards as evidence of how electronic records to be recorded or stored 6. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented [in any legal proceeding] 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 endeavor that used, recorded or stored the electronic record and the nature and purpose of the electronic record.
Affidavits — proof by 7. The matters referred to in subsection 4(2) and sections 5, and 6 may be established by an affidavit given to the best of the deponent's knowledge or belief. Sec 8. Cross-Examination Affidavits — Cross-examination on 8(1). A deponent of an affidavit referred to in Section 7 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced. 8(2). Any party to the proceedings may, with leave of the court, cross-examine a person referred to paragraph 5(c). 9. Repeal provisions which require retention of original after microfilming. (*e.g.*: Remove six year rule on retaining original documents after Microfilming)