Canadian Journal of Law and Technology

Volume 9
Number 1 *1 & 2*

Article 7

6-1-2011

Electronic Discovery- Sedona Canada is Inadequate on Records Management - Here's Sedona Canada in Amended Form

Ken Chasse

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/cjlt

 Part of the Computer Law Commons, Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Ken Chasse, "Electronic Discovery- Sedona Canada is Inadequate on Records Management - Here's Sedona Canada in Amended Form" (2011) 9:1 CJLT.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Law Scholars. For more information, please contact hannah.steeves@dal.ca.

Electronic Discovery — *Sedona Canada* is Inadequate on Records Management — Here's *Sedona Canada* in Amended Form

Ken Chasse[1]

INTRODUCTION

Introducing Records Management Compliance to Sedona Canada so that it can more Effectively Influence the Adequacy and Cost-containment of Electronic Discovery

Electronic discovery and "system integrity": whereas the integrity (reliability; truthfulness) of a paper record is dependent upon its own history, the integrity of an electronic record is dependent upon the integrity of its electronic records management systems (its ERMS). That is the "system integrity" concept of records reliability, *i.e.*, "records integrity" requires "systems integrity." Such is the fundamental nature of an electronic record — it is dependent for everything on its electronic records system. It is "systems dependent" for its existence, its integrity, and its accessibility. Therefore, this "system integrity" concept is the conceptual basis and rule of admissibility of the electronic records provisions in the Evidence Acts across Canada.[2] And it is part of the electronic commerce legislation.[3] And there-

---

1 Ken Chasse, J.D., LL.M., member of the Law Society of Upper Canada (Ontario), and of the Law Society of British Columbia, Canada.

2 See for example: Canada *Evidence Act* ("CEA"), R.S.C. 1985, c. C-5, ss. 31.1–31.8; (Ontario) *Evidence Act* ("OEA") R.S.O. 1990, c. E.23, s. 34.1; Alberta *Evidence Act* ("AEA"), R.S.A., 2000, c. A-18, ss. 41.1–41.8; (Nova Scotia) *Evidence Act* ("NSEA"), R.S.N.S. 1989, c. 154, ss. 23A–23.H. These electronic records provisions are reproduced as Appendix C to the article, Ken Chasse, "The Admissibility of Electronic Business Records" (2010), 8 Canadian Journal of Law and Technology 105 at 179–191. The Evidence Acts (or other "evidence" legislation) of twelve of Canada's 14 jurisdictions have electronic records provisions. The Evidence Acts of British Columbia and Newfoundland and Labrador do not yet have electronic records provisions. In British Columbia, the business records provisions in s. 42 of the *Evidence Act*, R.S.B.C. 1996, c. 124, would have to be used to determine the admissibility of electronically-produced records, a purpose for which they were not designed. The *Evidence Act*, R.S.N.L. 1990, c. E-16, of Newfoundland and Labrador does not have a business record provision. Therefore the business record exception to the hearsay rule at common law would have to be used, a purpose of which it has not yet been adequately interpreted.

3 The *Uniform Electronic Evidence Act* (UEEA) is in Appendix C of this article, and the *Uniform Electronic Commerce Act* (UECA) is in Appendix D. The UEEA is the model Act for the electronic records provisions, which accounts for their being almost exact copies of one another in the Evidence Acts across Canada. And the UECA has been similarly copied across Canada (the Northwest Territories does not yet have an UECA-type Act). Therefore those Uniform Acts are reproduced in those Appendices as representative of that legislation. Appendix B contains the statutory citations for the Evi-

fore it must be made the conceptual foundation of any law or series of principles governing electronic discovery, otherwise they will perform inadequately at best, if not fail. But *The Sedona Canada Principles — Addressing Electronic Discovery* ("*Sedona Canada*") provides neither analysis nor description of the relationship between electronic discovery and electronic records management systems.[4] Nevertheless, it is now the leading standard governing electronic discovery in Canada, and part of the enacted law and practice directions of electronic discovery.[5]

Because an electronic record in electronic storage is dependent upon its ERMS for everything, any standard governing electronic records, such as *Sedona Canada*, should be made compatible with authoritatively established principles of electronic records management. *Sedona Canada* isn't. Consequently, the *Principles* themselves in amended form (without their "Comments") constitute the last section of

---

dence Acts' electronic records and business record provisions, and the citations of the electronic commerce Acts, federal, provincial, and territorial.

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

And the companion text, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery*, available from The Sedona Conference, Working Group 7 series, October 2010; online: <http://www.thesedonaconference.org /dltForm?did=Canadian__Proportianality.pdf>

There are also, *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>. What is stated herein is equally applicable to this U.S. text, the two being very similar.

And the 2008 "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; online: <http://www.thesedonaconference.org/content/tsc_cooperative_proclamation/proclamation.pdf>.

And see the Australian Law Reform Commission's, *Managing Discovery — Discovery of Documents in Federal Courts*, Final Report March 2011; tabled in federal Parliament and released, May 25, 2011; online: <http://www.alrc.gov.au/ publications/managing-discovery-discovery-documents-federal-courts-alrc-report-115>. Or the ALRC's home page; online: <http://www.alrc.gov.au/>.

5 For example, the Ontario *Rules of Civil Procedure*, Rule 29.1.03(4) states: "Principles re Electronic Discovery — 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."

this article (before the four Appendices, A–D[6]). As they stand now, the principles of *Sedona Canada* may produce inadequate electronic discovery because they take no account of the vulnerability of electronic records to the state of the electronic records systems management they are subject to. As a result, *Sedona Canada* concerns fairness, but doesn't deal adequately with adequacy.[7] In the absence of procedural adequacy, there can be no certainty as to procedural fairness.

For example, the current "proportionality principle" of electronic discovery can easily be made a fraudulent defence for inadequate production and discovery in general if a party is not made accountable for the state of its records management.[8] The ways of corruptly using electronic technology and records management to render accessibility "disproportionately difficult," if not impossible, are of a great variety and number. Therefore all rules of discovery and the admissibility of evidence should include a power to hold parties accountable for their records management.

Discovery and evidence are interdependent — what is "discovered" is made available to be used as evidence, and the rules of evidence affect the scope of discovery. In turn, the principles of electronic records management must be based on the "system integrity" concept. Then, those principles can serve the needs of discovery and evidence. Those relationships establish a "triangle of interdependence," *i.e.*, the interdependence of electronic discovery, admissible evidence, and electronic records management. It is an interdependence that is fundamental to all three, and to everything that each of them can be.

To accept the principle that electronic records management must become an integral aspect of the law of electronic discovery, means that records management is not a mere facilitator of its application or helpmate for interpreting rules of discovery. At best, the legal literature on electronic discovery assigns records management and its standards[9] that lower "facilitator and helpmate" function and not that

---

6 The Appendices herein are: A — Summary of the electronic records management system compliance standards established by the National Standard of Canada *Electronic Records as Documentary Evidence* CAN/CGSB-*72.34*-2005; B — List of the electronic records and business record provisions in the Evidence Acts, and of the electronic commerce Acts; C — *Uniform Electronic Evidence Act*; and, D — *Uniform Electronic Commerce Act*. These "Uniform Acts," being the "model Acts" from which their federal, provincial, and territorial legislated progeny were copied.

7 The Preface to *Sedona Canada* states of electronic discovery (at p. i): "It requires universal understanding by the Canadian Bar and a common approach rooted in proportionality and reasonableness, with respect for variations in local rules and practices." That is a statement as to fairness but not adequacy.

8 Proportionality: see, *Sedona Canada*, *supra* note 4, and, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery*, *supra* note 4. But there is no reference to the principles and standards of records management in either text, even though their principles are dependent for their adequacy and effectiveness upon the state of the parties' electronic records management systems (ERMSs). Electronic discovery's cost-containment is also affected by the state of records management.

9 The National Standards of Canada are: (1) *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("*72.34*"), published in December 2005; and, (2) *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93

of an integral aspect of the law of discovery.[10] Electronic records management is the factual foundation of all laws concerning electronic records.

The "system integrity" concept constitutes the admissibility provision of the electronic records provisions of the Evidence Acts in Canada. And it should be an integral aspect of any other admissibility provision used for electronic records. To an equally necessary extent, the "system integrity" concept should be written into *Sedona Canada*, not only to provide for the adequacy of electronic discovery, but also to provide rules for controlling its cost.[11]

("*72.11*") (first published in 1979 as, *Microfilm as Documentary Evidence*). (*72.34* incorporates all that *72.11* deals with and is therefore the more important of the two. Because of tis age, *72.11* should not be relied upon for its "legal" content. However *72.11* has remained the industry standard for "imaging" procedures — converting original paper records to electronic storage.) These standards were developed by the CGSB (Canadian General Standards Board), which is a standards-writing agency within Public Works and Government Services Canada (a department of the federal government). It is accredited by the Standards Council of Canada as a standards development agency. The Council must certify that standards have been developed by the required procedures before it will designate them as being National Standards of Canada. *72.34* incorporates by reference as "normative references," many of the standards of the International Organization for Standardization (ISO) in Geneva, Switzerland. ("ISO," derived from the Greek word *isos* (equal) so as to provide a common acronym for all languages. See also notes 41–43 *infra* and accompanying text). The process by which such national standards are created and maintained in Canada is described within the standards themselves (reverse side of the front cover), and on the CGSB's website (see, "Standards Development"), from which website these standards may be obtained; online: <www.ongc-cgsb.gc.ca>.

See also the list of American and ISO standards cited in footnote 53 on page 37 of the book by, David Wotherspoon and Alex Cameron, (General Editor: Sunny Handa), *Electronic Evidence and E-Discovery* (LexisNexis Canada Inc., 2010). And see also this standard, *Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology* ANSI/AIIM TR31, being a standard of the American National Standards Institute and of the Association for Information and Image Management. Although authoritative, not having been developed by a Canadian standards development agency such as the CGSB, such standards have not been approved and designated by the Standards Council of Canada as comparable to a National Standards of Canada. A statement of the "operations" of the Standards Council of Canada in relation to standards can be obtained from its website; online: <http://www.scc.ca/en/about-scc/operations>.

10 Consider this statement concerning the use of the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005: "Complying with this standard will not only provide useful guidance in terms or what to cover in a document management policy, it will also help ensure that electronic information is admissible in court." It appears at page 39 of the book by David Wotherspoon and Alex Cameron (General Editor: Sunny Handa), *Electronic Evidence and E-Discovery* (LexisNexis Canada Inc., 2010).

11 The "Introduction" to *Sedona Canada* contains this paragraph about the cost of electronic discovery (p. 5): "Early experiences in Canada with e-discovery have been marked by very expensive and time-consuming burdens in preserving and producing electronically stored information in litigation. We have heard anecdotal stories about

As to adequacy, records management is not a mere helpmate of electronic discovery; it is its factual foundation. Therefore the law should incorporate and apply the fact that electronic records depend for everything on their electronic records systems. The "system integrity" test of admissibility of the electronic record provisions of the Evidence Acts says that, and so should the principles, rules, and laws of electronic discovery.

A paper record can exist without its records system; an electronic record cannot.[12] To use, corrupt, or destroy a paper record, one needs physical access to the records system wherein it is stored. But to use, corrupt, or destroy an electronic record one merely needs electronic access to its records system, from anywhere. Therefore any set of rules or principles for controlling the use of electronic records for any purpose, including electronic discovery, should incorporate the established policies and practices of electronic records management.

As to cost, rules of electronic discovery are needed with which to punish parties with "sanctions"[13] for not maintaining their electronic records systems in compliance with authoritative standards of electronic records management — to sanction when inadequate records management interferes with electronic discovery or otherwise damages parties' interests. Such compliance greatly reduces the cost of, and increases the effectiveness and fairness of doing anything that can be done with electronic records.[14] Therefore, by thus incorporating records management into the law of electronic discovery, discovery is made more effective and is better equipped to control its costs.[15]

---

cases where parties were required to spend millions of dollars to process and review large volumes of electronically stored information that had marginal relevance to the case. In other cases, the preservation of electronically stored information has been costly, necessitating the restoration of thousands of backup tapes containing only marginally relevant information. In other cases, counsel simply ignore electronically stored information as a potential source of evidence."

12 An electronic record can exist outside its electronic records system by being printed out on paper, microfilm, or other media of storage. But those are electronically-produced records, and not records in electronic form. However, the term "electronic record" is commonly used in reference to both.

13 See *Sedona Canada* Principle 11 as to the definition and use of "sanctions" below at p. 162.

14 Electronic discovery is but one of several reasons for establishing an educational and licensing body for creating and regulating professional certifiers of compliance of records systems with established standards of electronic records management, particularly the National Standards of Canada — see *supra* note 9, and *infra* note 32. See also the section on certification, section VII below (p. 151).

15 The present cost of electronic discovery aggravates the "access to justice" issue. For example, view the video of the University of Toronto, Faculty of Law's *Access to Civil Justice Colloquium*, on Feb. 10, 2011; online: <http://hosting.epresence.tv/MUNK/1/watch/219.aspx> The video provides seeing and hearing the Chief Justice, Beverley McLachlin C.J.C., as the keynote speaker (introduced by Ontario's Attorney General, Chris Bentley). She has spoken publicly "off the bench," several times on this topic — the legal profession has a monopoly on the provision of legal services, therefore it has a duty to make legal services available at reasonable cost.

The "Foreword" to *Sedona Canada*, written by Justice Colin Campbell of the Superior Court of Justice of Ontario, and Justice J.E. Scanlon of the Supreme Court of Nova Scotia points out that, "electronically stored information is rapidly becoming a feature of even the most routine of civil cases as well as cases in family and criminal litigation."[16]

However, relying on "proportionality," unsupported by the express sanctionability of faulty electronic records management, is but a good intention without hope of power to discipline.[17] Electronic records management is much more complex and demanding for the greater capacities it provides beyond traditional "paper" records management. Such greater capacity includes the ways the parties may be fraudulent in discovery.

Therefore, the third consequence of the necessary introduction of records management to the law of electronic discovery (in addition to its effect upon the adequacy and cost of electronic discovery) is the enforcement of a general duty to maintain records systems in compliance with authoritative standards of electronic records management. Privilege brings duty. The privilege of driving a motor vehicle imposes the duty of "documenting" oneself with driver's license and proof of insurance. A somewhat more onerous records management duty befalls lawyers in the private practice of law. A failure to keep proper records is a failure to meet standards of professional competence, a disciplinary offence.[18] Similarly, the privi-

---

16 *Sedona Canada*, *supra* note 4 at page *ii*. The full paragraph states: "There continues to be a misconception that e-discovery issues are mainly applicable to big law firm, large document cases. Electronically stored information is rapidly becoming a feature of even the most routine of civil cases as well as cases in family and criminal litigation. The cost of dealing with e-discovery issues in some cases exceeds the amount in issue." Justices Campbell and Scanlan are listed (at pp. 41-42) as members of the "Steering Committee and/or Editorial Committee" of the Sedona Working Group 7 that wrote *Sedona Canada*.

17 See: The Honourable Colin J. Campbell (2010), 28 Advocates' J. No. 4, 4–8, at para. 39: "At the most simplistic level, proportionality in the disclosure and production of documents should require that the information be reasonably accessible admissible evidence in support of a plausible cause of action." And, without the threat of penalties for not maintaining "accessibility" by way of good records management that maintains the "integrity" of electronic records and the "integrity" of the electronic records systems that contain them, (as required by the "admissibility test" of the electronic records provisions of the Evidence Acts), a party can falsely claim that key records are no longer "accessible."

18 The (Ontario) *Law Society Act*, R.S.O. 1990, c. L.8, s. 41 provides (in relevant part) that, "A licensee fails to meet standards of professional competence for the purposes of this Act if, (a) there are deficiencies in, . . . (iii) the records, systems or procedures of the licensee's professional business, or (iv) other aspects of the licensee's professional business; and (b) the deficiencies give rise to a reasonable apprehension that the quality of service to clients may be adversely affected." However the Rules of Professional Conduct, Rule 2.01 "Competence," states (in relevant part): "2.01(1) 'competent lawyer' means a lawyer who has and applies relevant skills, attributes, and values in a manner appropriate to each matter undertaken on behalf of a client including . . . (e) performing all functions conscientiously, diligently, and in a timely and cost-effective manner, ..."

leges the general population has gained through electronic technology means a greater need for more sophisticated disciplining of records management. Each new use of electronic technology requires new legislation, *e.g.*, legislation as diverse as that for the laws of evidence, electronic commerce, personal information protection and privacy, electronic discovery, taxation, electronic signatures, securities, and online dispute resolution.[19] In turn, each new legislated Act creates an additional need for the keeping of electronic records, or facilitates and motivates their greater production and use, *e.g.*, legislation facilitating electronic commerce and mobile communications, *inter alia*, because every electronic communication, transmission, and submission creates an electronic record. Therefore almost all disputes and their litigation and arbitration involve electronic records. As a result, increasing the privileges and capacities brought by electronic technology must increase the enforcement of standards for records management.[20] That means that records management is now much more often a matter of "legal compliance," and much less often merely "a good business practice," *i.e.*, a necessary and integral aspect of the law and not merely its facilitator. The Principles of *Sedona Canada* should be amended to so provide — so as to provide better for the adequacy and cost of electronic discovery.[21]

Therefore the necessary train of principles to be set in motion for an adequate and effectively cost-containing law of electronic discovery is: "system integrity" as the basis of electronic records management, in turn the basis of rules of admissibility and electronic discovery, and in turn requiring the enforcement of authoritatively principled records management. In contrast, the current approach to electronic discovery takes no account of this necessary reality, nor of the fundamental nature of an electronic record and the requirements that, that nature dictates for records management. It is based entirely upon inadequately defined principles of fairness and "being reasonable and proportionate" — inadequately defined because they are not rooted in the fact that electronic records depend for everything upon their records systems. If not challenged, bad records management can enable demands for further production to be opposed as being "disproportionate."

---

19 See the proposals in the U.N.'s UNCITRAL *Report of Working Group III (Online Dispute Resolution)* on the work of its twenty-second session (Vienna, 13–17 December 2010); online: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V11/801/48/PDF7/V1180148.pdf?OpenElement>

20 See the discussion of "sanctions" for a party's faulty electronic discovery below in section V (p. 148), "Analysis in *Sedona Canada* of Records Management Policies, Practices, and Standards," and in relation to "Amended Principle 11" in section X (p. 156), "Amending the Sedona Canada Principles to Include Records Management."

21 A profession of experts trained in certifying the compliance of electronic records management systems with established, authoritative principles of electronic records management will provide substantial "systemic" support and infrastructure to the law of discovery's sanctioning inadequate records management. But the lack of funding has prevented a standards development agency of government from creating such a certification system. Government has to be persuaded that such is needed to make the law and practice of discovery operate adequately and at a reasonable cost. See also section VII below, "A Certification Procedure for Records Management Standards Compliance," at p. 151.

The "Preface" to *Sedona Canada* states of electronic discovery:[22] "It requires universal understanding by the Canadian Bar and a common approach rooted in proportionality and reasonableness, with respect for variations in local rules and practices." But what is *Sedona Canada's* use of "proportionality and reasonableness" in regard to accessing relevant records from electronic record systems rooted in? Apparently, nothing! What is the conceptual foundation? How to apply them with "an even hand" from case to case?

Far better to flesh out the definition, requirements, and limitations of "system integrity" than to rely on indefinite words such as "proportionality and reasonableness." But if they have to be used, root them in the reality of the high quality electronic records management "system integrity" requires. It is not too much to have the law require, given the considerable demands that electronic technology is already having legislation make of records management.

Even if the electronic records provisions were not in the Evidence Acts, the same requirements of the "system integrity" concept for adequate records management apply. They apply in provinces such as British Columbia and Newfoundland and Labrador, even though their Evidence Acts do not yet contain electronic records provisions. The need to make records management an integral part of the laws and principles of electronic discovery arises not from the laws of evidence concerning electronic records. It arises from the nature of electronic records and the quality of records management they make necessary for their continued existence, integrity, and accessibility.[23]

I. ELECTRONIC RECORDS IN ELECTRONIC RECORDS SYSTEMS ARE LIKE DROPS OF WATER IN A POOL OF WATER

Electronic records are not like paper records, but rather like drops of water in a pool of water. We cannot define or describe an electronic record in an electronic record system by describing the history of a particular group of electrons, no more than we can describe the history of a drop of water after it falls into a pool of water. When drops of water later emerge from the pool of water, we cannot associate any of them with particular drops that entered the pool of water. That points out the critically important difference between traditional "paper" records management and electronic records management. A paper record maintains its physical, corporeal existence and identity while in its records system. Therefore the reliability of a paper record can be proved by proving its own particular history from its creation until it is adduced as evidence in a court, quite apart from the reliability of its record system. But an electronic record does not maintain its existence as a particular group of electrons in its records system, no more than a drop of water maintains its existence and identity in a pool of water. The molecules of the drop of water are subject to everything that happens to the pool of water. To prove the fate of any

22 *Supra* note 4 at p. i.

23 All of which should cause law firms to develop "records management lawyers," and "records management practice groups," because electronic records and electronic records management are now a very major part of the factual foundation that gives rise to the application of laws to human activity.

drop of water requires proof of what has happened to the pool of water, *e.g.*, the purity of any drop in the pool of water requires proof of the purity of the pool of water as a whole. Similarly, once an electronic record is entered into an electronic records system, it is subject to everything that happens to that electronic record system and can possibly happen to that system, including its state of standards-compliance, security, and vulnerability to the Internet. It can be accessed, but remains subject to the state of its records system, and to the motivations, competence, and character of anyone who can get electronic access to it.

II. AN ELECTRONIC RECORD IS NO BETTER THAN THE ELECTRONIC RECORDS SYSTEM IN WHICH IT IS RECORDED OR STORED

It should follow that if one must prove the worth of a "system" as a condition-precedent to admissibility, one should have to make disclosure of the means by which its "system integrity" is proved.[24] There is no valid argument that proving the "system integrity" of an electronic record requires merely proof of the "system integrity" of that part of the records system in which the record existed. Every record and its records system are part of the same, single electronic "pool." However, if parts of an organization's records operations are sufficiently independent in operation, management, structure, and purpose, such parts may each constitute an "electronic records system" for purposes of proving "system integrity," and therefore the admissibility of any particular electronic record. For example, an "imaging" department (for scanning paper-original documents into electronic storage) may be sufficiently apart in function and purpose from the rest of an organization's records management operations as to be a separate "system" for purposes of the "system integrity" test. And certain financial functions may operate in specialized and separate divisions as to be arguably separate "systems." And therefore there is no valid argument that the "system integrity" test of admissibility is unworkable because it requires proof of the integrity of all of an organization's local, national or international records management operations in order to use a single printout as evidence.

III. THE COMMON DEFECTS OF ELECTRONIC RECORDS MANAGEMENT SYSTEMS THAT UNDERMINE DISCLOSURE AND DISCOVERY

Electronic discovery, examination on discovery, and cross-examination can reveal the serious defects in the management of electronic records systems to show the state of records management "system integrity." Among the most common defects, routinely found in the systems of large organizations, including those of government departments and agencies, universities, public utilities, and commercial or-

---

24 The presumptions in these Evidence Acts, *supra* note 2: s. 31.3 CEA; s. 41.5 AEA; s. 34.1(7) OEA; and, s. 23E NSEA, do not alter this requirement. Proof of their conditions-precedent will make necessary the same level of production. And, production by the proponent of admissibility is necessary if the "evidence to the contrary" mechanism is to be meaningful — the opponent of admissibility cannot investigate "system integrity" when there is no access to the system.

ganizations are these:[25]

- the extent of the records holdings is not known;
- records are neither 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);
- 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

25 This list of defects comes from the records management experts I have worked with.

(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[26]
- "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;[27]
- inadequate compliance with the records management requirements of the privacy laws;[28]

---

26 The national standard, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("*72.34*"), *supra* note 9, uses the term, "Corporate records officer (CRO)." See also note 76 *infra*.

27 The ninth in the list of points in proof of "system integrity," specified in the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 (*supra*, note 9) 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 disposition [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 [*i.e.*, a "disaster recovery" plan for fire, flood, mishandling, sabotage and similar system vulnerabilities].

28 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 the 13 other jurisdictions of Canada except for the Northwest Territories (*i.e.*, 10 provinces plus 3 territories)), and Part 3,

- 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.

That there may in fact be such defects is ignored in discovery procedures. Various pieces of an electronic records system are demanded, such as, records, metadata, email, and storage devices, but there is no demand for proof of records management reliability and "integrity." Electronic discovery is conducted without a records management audit or comparable certification of records management quality. The above defects can result in: (1) relevant records not being available; (2) inadequate discovery; and, (3) inadmissibility, or the absence of the necessary "weight" that gives records the appearance of sufficient reliability. *Sedona Canada* is without Principle or Comment on such facts and the uses of electronic discovery they should engender. Therefore for example, without an assessment of the state of a records system, one cannot say which demands are "disproportionate" in regard to that system (*Sedona Canada* Principle 2), and which records are "reasonably accessible" (Principle 5). And a duty to inform early as to relevant deleted or residual data (Principle 6), depends on what practices and controls exist in regard to such data in the management of each records system. And the alleged limits of a records system can be contrived to place relevant records, perceived to be damaging to one's interests, into another records system, perhaps making necessary further proceedings.

However, an independent certification of "system standards compliance," or sworn statement to same effect by a chief records officer, subject to examination, could remove such issues from contention. In other words, the state of records management determines the relevance and manner of application of the Principles of *Sedona Canada*. Therefore it should be amended to make records management an integral aspect of its application.

If an ERMS has such defects, a disclosure request as simple as, "produce all records on subject X," cannot be 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 Rules of Civil Procedure and in *Sedona Canada*. One has to know one's records management 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 a records management system is not kept or demanded by an opponent. A records management system should be regularly "internally audited," and periodically independently, "externally audited."[29]

"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).

29 This process provides a thorough system analysis and comprehensive certification of compliance with the two National Standards of Canada, *supra* note 9. But a quicker and less expensive procedure is needed for certifying such "systems compliance" for

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.[30] 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.[31] 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.

An ERMS having the above defects cannot comply with the "prime directive" of the national standards: "An organization shall always be prepared to produce its records as evidence."[32] Compliance with it is an indicator of the state of overall compliance with the national standards. When the "prime directive" cannot be satisfied, a chief records officer cannot assert in good faith, that a comprehensive, accurate, and precise search of its records holdings is possible. In turn, an ERMS cannot comply with the "system integrity test" by which the admissibility of electronic records is to be determined, nor provide adequate discovery and production.[33] Therefore clients, before they are parties, need to have their ERMSs ready

---

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, should establish educational courses for records management specialists to become licensed, or otherwise official certifiers. See the discussion of this proposal in section VII below (p. 151), "A Certification Procedure for Records Management Standards Compliance."

30 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

31 A "full substantive audit" is used when Internal Controls are weak such that the auditor cannot place reliance on them. There are two kinds of "substantive testing": Analytical and Direct Testing of balances and underlying transactions. Analytical testing is less reliable so it is generally used where there are strong Internal Controls. Direct testing of balances and underlying transactions is required when Internal Controls are weak. In essence the cost of having weak Internal Controls is higher "audit risk," and therefore, higher costs because Direct Testing is more time consuming than Analytical Testing. "Audit risk" is the risk that the auditor will fail to discover material misstatement in the financial statements and that users will place reliance on these statements to their detriment.

32 *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 9.

33 There are many specific compliance tests that records management project teams can apply to determine the level of compliance of a records system with the national standards, *Electronic Records as Documentary Evidence*, and the earlier national standard,

for discovery demands for proof of compliance with the "prime directive" of the National Standards of Canada for electronic records management.

IV. LEGAL COMPLIANCE

Records systems now exist in an environment of "legal compliance" — they must comply with the many laws that make demands of them and are dependent upon them in order for those laws to operate properly, and in compliance with the authoritative standards of records management.[34] No longer is it sufficient for a records system to be operated according to "good business practice." That is the concept underlying the "usual and ordinary course of business" test of admissibility contained in the business record provisions of the Evidence Acts.[35]

Clients should be advised:

> (1) to have their records systems prepared to produce records as evidence and for electronic and "paper" discovery at all times;
>
> (2) to require their records managers to be prepared at all times to give evidence as to the state of their records systems; and,
>
> (3) advised of the importance to issues of discovery and admissibility of evidence of compliance with the National Standards of Canada as to electronic records management.

The defects listed in section III above, can render uncertain the comprehensiveness, accuracy, and precision of electronic discovery — most of them can do so alone, as well as in combinations. And therefore they: (1) reduce the cost-efficiency of performing electronic discovery; (2) diminish the completeness and quality of the evidence that is records; and in turn, (3) they affect the efficacy of the law. The "triangle of interdependence" makes discovery and evidence no more reliable and efficient than its weakest link. It is of critical importance to the reliability of records as evidence.

V. ANALYSIS IN *SEDONA CANADA* OF RECORDS MANAGEMENT POLICIES, PRACTICES, AND STANDARDS

There is none. The most extensive reference in *Sedona Canada*[36] to records management is in relation to Principle 11, which deals with sanctions for, "failure to meet any obligation to preserve, collect, review or produce electronically stored information." The subsection with the heading, "Comment 11.e. Reasonable

---

Microfilm and Electronic Images as Documentary Evidence CAN/CGSB-72.11-93, *supra* note 9. The resulting report indicates the level of compliance found by each test, along with recommendations, and a legal assessment as to "legal compliance" with legislated records and records management requirements and consequences.

34 "Legal compliance" with laws, for example, concerning evidence, electronic commerce, personal information and privacy protection, and tax laws.

35 The business record provisions are listed in Appendix B, *infra*. The underlying principle is that the "profit motive," as represented in the admissibility test, "the usual and ordinary course of business," will ensure good records management, otherwise, the information necessary for good business decisions will not be available.

36 *Supra* note 4.

Records Management Policies,"[37] discusses not the need for records management policies as a necessity for cost-efficient and effective electronic discovery, but rather the defense against sanctions as to having destroyed records by reason of having followed a "reasonable records management policy." The subsection begins:

> Compliance with a reasonable records management policy, or justifiable inadvertent destruction or non-production of relevant documents should not, in the ordinary course, constitute sanctionable conduct.

ERMS policies should not be merely "reasonable"; they must be compliant with established standards of records management — the objective standards of the records management profession in place of the subjective "reasonableness" of the legal profession. No part of *Sedona Canada* discusses records management policies and practices in general, nor the dependence of electronic discovery upon records management. As a result, also missing is a discussion of sanctions for a party's failure to maintain its records system in compliance with authoritative standards of electronic records management where such failure causes damage or procedural prejudice to other parties. Such limiting of the scope of sanctions to intentional, reckless, or otherwise negligent failures to perform specific duties of electronic discovery will not bring enforcement and support to that much more important need for "records management standards compliance." Even though a "discovery failure" is unintentional, inadvertent, and not due to any specific error or omission, but rather caused by faulty records management, it should nevertheless be sanctioned. Pleading the "honest defense" that says, "I tried very hard to get the records, but they just are not there," should provide no defense. Such failures are serious not simply because of damage or prejudice caused, but more so because they will be repeated by others.

Many organizations function quite well (in their own opinions, and required level of performance), with seriously faulty records systems in perpetuity.[38] The necessary time and resources to "fix" such systems are pre-empted by other priorities and the excuse, "well, we've had no trouble before." "No trouble before" only because they have not been challenged before. If such organizations perform electronic discovery badly, to the detriment of opposing parties, they should be made to endure a penalty, instead of enjoying faulty records management as a defence against having to make adequate and fair electronic discovery.

VI. SYSTEMS" CONCEPTS VERSUS "RECORDS" CONCEPTS: THE ELECTRONIC RECORDS AND BUSINESS RECORD PROVISIONS IN THE EVIDENCE ACTS

The "system integrity" test is an objective test, whose meaning and application can be determined by established, authoritative standards such as the National Standards of Canada for electronic records management.[39] For example, the national

37 *Ibid.* at 36.

38 See the list of "Common Defects of Electronic Records Management Systems that Undermine Disclosure and Discovery," in section III above (p. 143).

39 *Supra* note 9.

standard, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("72.34"), defines the key word "integrity" this way:[40]

> NOTE 1 The term "integrity" is used in the electronic records provisions of the Evidence Acts in the phrases "the integrity of the electronic records systems" and "the integrity of the electronic record." However, the term integrity is not defined. In the absence of a statutory or judicially created definition, the principles of this standard shall serve as an operational definition of the word integrity used in the Evidence Acts.

In turn, these standards are partially based upon the international standards of the International Organization for Standardization ("ISO") in Geneva, Switzerland, thus forming an integrated web of objectively and authoritatively based standards.[41] Canada's national standards have been approved and certified by the Standards Council of Canada as national standards, and they have incorporated by reference, as "normative references," the ISO standards concerning electronic technology, information technology, information processing, and data processing.[42] Therefore the "system integrity" test is to be applied by determining the state of compliance of an adduced record's electronic record system with those National Standards of Canada. They state the basic, minimal requirements of adequate electronic records management. At present, 72.34 is the most authoritative standard in Canada that can give the "system integrity" test meaning and content[43] — *e.g.*, with which to answer questions such as: (1) what are the requirements for proving

---

40 *Supra* note 9, at p. 9, clause 3.34, defining "Integrity." To further declare the interdependence of this national standard and the electronic records provisions of the Evidence Acts (which contain the "system integrity" rule of admissibility) the standard adopts the *Uniform Electronic Evidence Act* (the UEEA) as a "normative reference" (in subsection 2.5, page 3). The UEEA is the model Act for all of the electronic evidence provisions in Canada. It is reproduced in Appendix C (at p. 169).

41 *Supra* note 9 (*Electronic Records as Documentary Evidence*). In section 2, "Normative References," on pp. 2–4, several ISO standards and other Canadian standards are listed under this introductory statement: "2.1 The following referenced documents are indispensable in the application of this document." The ISO website states of the acronym "ISO": "Because 'International Organization for Standardization' would have different acronyms in different languages ('IOS' in English, 'OIN' in French for *Organisation internationale de normalisation*), its founders decided to give it also a short, all-purpose name. They chose 'ISO', derived from the Greek *isos*, meaning 'equal'. Whatever the country, whatever the language, the short form of the organization's name is always ISO." See; online: < http://www.iso.org/iso/about/discover-iso_isos-name.htm>.

42 *Ibid.*, subsection 2.6 at p. 3 of the national standard, *Electronic Records as Documentary Evidence*, *supra* note 9, contains a list of the ISO standards that it has incorporated as normative references.

43 There are other standards such as American and ISO standards (see the references in note 9 *supra*). Although authoritative, those standards, not having been developed by a Canadian standards development agency such as the CGSB, have not been approved and designated by the Standards Council of Canada as comparable to a National Standard of Canada. Therefore the National Standards of Canada for electronic records management are the most authoritative standards available in Canada for interpreting and applying legislation in Canada. They are referred to in the following notes and their accompanying texts: *supra* notes 9, 10, 26, 27, 32, and 33. A statement of the

the "integrity" of a system; (2) what defines and delimits a "system" — can it be a division or a branch office of an organization's records management operations? In preparation for gathering and adducing evidence, and for opposing admissibility, electronic discovery can be used to investigate the "system integrity" of any ERMS involved.

In contrast, the "usual and ordinary course of business" test of the business record provisions of the Evidence Acts[44] is a completely subjective test — each business determines its own "usual and ordinary" state of records management. If very inadequate, unreliable records management is the product of an organization's "usual and ordinary course of business," its records must be admitted into evidence once proved to have been so made.[45]

VII. A CERTIFICATION PROCEDURE FOR "RECORDS MANAGEMENT STANDARDS COMPLIANCE"

Formal certification by a professionally licensed certifier, of an ERMS's compliance with authoritative standards of compliance would make the processes of adjudicating issues as to the adequacy of discovery, and the admissibility of electronic records as evidence, much easier. Such certification would provide sufficient evidence in proof of the "system integrity" of any ERMS, thus removing the need to argue and adjudicate such issues. At present, such certification requires the investigation and report of a records management expert and a legal assessment as to compliance. It is also done as a part of projects that involve making recommendations requiring substantial alterations to large ERMSs. Such projects can produce a succession of large reports concerning analysis, recommendations, and policy and procedures development, including drafting various records management manuals and protocols. But this solution is not practical for the thousands of court cases that

---

"operations" of the Standards Council of Canada in relation to standards can be obtained from its website; online: <http://www.scc.ca/en/about-scc/operations>.

44 The Alberta and Newfound and Labrador Evidence Acts do not have a business record provision. The common law exception to the hearsay rule for business records would apply. See the list of business and electronic records provisions in Appendix B below.

45 There is an argument that s. 30(6) CEA provides an additional admissibility rule for federal proceedings, which is dominant over s. 30(1) CEA. But this "circumstances of the making" provision should give the same result. The comparable provision under the provincial Evidence Acts goes to "weight," not admissibility. See: Ken Chasse, "Electronic Records as Documentary Evidence," (2007), 6 Canadian Journal of Law and Technology 141 at 149-150. An electronic business record, to be admitted into evidence, has to satisfy both business record and electronic record provisions of the Evidence Acts. Although the latter concern the best evidence rule and authentication issues, and the former the hearsay rule issues, evidence that satisfies the electronic record provisions should by definition ("system integrity"), be judged as being sufficient for the latter. The business record provisions establish a statutory business records exception to the rule against hearsay evidence. The electronic records provisions establish an exception to the best evidence rule. For arguments that the best evidence rule is best abolished and inappropriate for issues concerning electronic records, see: Ken Chasse, "The Admissibility of Electronic Business Records" (2010), 8 Canadian Journal of Law and Technology 105 at 138.

use records as evidence every day. Needed is a certification process having a single-minded purpose to produce accurate certifications quickly and economically. Evidence of standards-compliance could then be given by affidavit, comparable to the affidavit for production of banking records provided by the "banking record" provisions of the Evidence Acts, banks being very often "third party record holders" of records relevant to proceedings to which they are not a party.[46] Affidavit evidence may substitute for testimony (*viva voce* evidence) once the use of such certifiers has a favourable forensic "track record," just as certificate evidence has replaced the testimony of police breathalyzer officers in every impaired driving and "over 80" case. Expert certifiers could be employed by the party adducing the electronic records, as well as by chief records officers wanting an independent certification of compliance. Also, such a certification system would facilitate providing proof that a records system can satisfy the environment of "legal compliance" applicable to all electronic records systems now.[47]

Other systems, equally dependent upon high quality electronic records management, use certification to ensure quality. For example, in regard to certifying compliance with the *Model Code for the Protection of Personal Information*, made mandatory by s. 5 of the *Personal Information Protection and Electronic Documents Act*,[48] there are professional auditors whose work relates to that of the Office of Privacy Commissioner of Canada.[49] And similarly, established certification processes exist for the standards of the ISO.[50] And for smaller records systems, their chief records officers should be able to provide comparable evidence of "'legal' and standards compliance." However, independent, professionally-licensed certification has the credibility advantages of being independent and authenticated by professional licensing.

The CGSB (Canadian General Standards Board),[51] should be given the resources to establish a project for educating and licensing expert certifiers, trained by the CGSB and officially designated as such. They could provide: (1) certifications of compliance with the CGSB's National Standards of Canada for electronic records management; and, (2) *viva voce* and affidavit evidence as to the requirements of the national standards, and as to the state of any particular records system

46 See for example, s. 29(2) CEA, and the affidavit provided in the electronic record provisions: s. 31.6 CEA; ss. 41.7, 41.8 AEA; s. 34.1(9), (10) OEA; and, ss. 23G, 23H NSEA.

47 See, Ken Chasse, "Electronic Records in the Criminal Court System" (2010), 14 Canadian Criminal Law Review 111 at 147–150, under the heading, "8. RIM Law is an Integrated System of 'Legal Compliance'." "RIM" means, records and information management.

48 S.C. 2000, c. 5 ("PIPEDA").

49 Online: <http://www.priv.gc.ca/>.

50 *Supra* notes 9 and 41; online: <http://www.iso.org/iso/about.htm.>

51 An agency of the federal government within Public Works and Government Services Canada, *supra* note 9. The CGSB developed the two existing National Standards of Canada concerning electronic records management: *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005; and, *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93, *supra* note 9.

in regard to compliance with those standards. The major resources necessary for such a profession and professional certifiers already exist in that the CGSB owns the property rights to the national standards, and there are experts in records management who currently work independently, providing advice as to the analysis and alteration of records systems.[52]

VIII. THE USE OF STANDARDS OF "SYSTEM INTEGRITY" IN APPLYING THE LAWS OF ADMISSIBILITY AND ELECTRONIC DISCOVERY

How to make authoritative standards of electronic records management an integral part of the laws as to the admissibility and discovery of electronic records, and not merely of optional assistance? Court decisions can do that by way of the sources they cite in interpreting the requirements of the "system integrity" test of admissibility of the electronic records provisions of the Evidence Acts.[53] If admissibility requires proof of records management "system integrity" as defined by the standards, then disclosure and production of such evidence will have to become a routine requirement of electronic discovery. But there are no decisions that define "system integrity," even though the electronic records provisions have been operative since 2000.[54] Those sections do not make the use of standards in the interpretation and application of the "system integrity" test mandatory,[55] but they are ex-

52 The existence of such certifiers would aid in "buffering" the CGSB's potential liability for damage allegedly caused by its standards. Just as drug manufacturers use doctors as experts and "knowledgeable intermediaries" operating between themselves and the patients allegedly damaged by their drugs, to shift or share liability, so such certifiers would provide a similar partial protection from liability by way of a networked warning system as to reported defects.

53 For example, s. 34.1(5), (5.1) OEA state: "(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. (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 integrity of the electronic record." Subsection (6) is the "relied upon printout" provision. It states: "An electronic record in the form of a printout that has been manifestly 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."

54 The first, ss. 31.1–31.8 CEA, became operative on May 1, 2000, as Part 3 of the *Personal Information and Protection of Documents Act* (PIPEDA), *supra* note 28.

55 An example of a standard of mandatory application is the, "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information," in Part 1 of PIPEDA (*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 5 and Schedule 1, Canadian Standards Association, Q830-96). The electronic records provisions of the Canada *Evidence Act*, R.S.C. 1985, c. E-5, ss. 31.1–31.8, were enacted by Part 3, ss. 56 and 57.

pressly made applicable. The "use of standards" provisions state:[56]

> 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.

Such evidence of standards, *etc.*, should be relevant even without this provision. However, its presence in the Evidence Acts should remove any issue or doubt as to the relevance and admissibility of standards, and perhaps alter the evidence needed for authentication of a standard.

Such standards deal with ***how*** electronic records are kept and not just with ***where*** they are kept. Legal literature should deal with both. For example, under the heading, "Unique Challenges of Electronic Discovery," an American attorney tells why lawyers have to become more knowledgeable about electronic information systems, but cites only the "**where**" and not the "**how**":[57]

> 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: 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 (log-ones/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.

---

56 This is the wording used in, for example, s. 41.6 AEA; s. 34.1(8) OEA; and, s. 23F NSEA. Section 31.5 CEA uses the same wording, the only significant difference being that the word "document" is used instead of "record." The electronic records provisions of the Evidence Acts of Alberta (AEA), Nova Scotia (NSEA), Ontario (OEA), and those of the Canada *Evidence Act* (CEA), along with the *Uniform Electronic Evidence Act* (UEEA; it being their "model Act" source) appear in the "Legislation Grids" as Appendices to these articles: Ken Chasse, "The Admissibility of Electronic Business Records," (2010), 8 Canadian Journal of Law and Technology 105 at 179–193; and, Ken Chasse, "Electronic Discovery in the Criminal Court System," (2010), 14 Canadian Criminal Law Review 111 at 169–180. For Quebec, comparable provisions are contained in Articles 2831–2842, 2859–2862, 2869–2874 of the *Civil Code of Quebec*, S.Q. 1991, c. C-64, to be read in conjunction with, *An Act to Establish a Legal Framework for Information Technology*, R.S.Q. 2001, c. C-1.1, ss. 2, 5–8, and 68. The UEEA is reproduced as Appendix C below (at p. 169).

57 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.

> 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.

But this passage does show: (1) not only an understanding of the close relationship between knowledge of ERMS 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 (the (U.S.) Federal Rules of Evidence) and the new (U.S.) Federal Rules of Civil Procedure for electronic discovery. Changes to either will cause changes to the other, in both content and interpretation.

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 Survey of American Law as follows:[58]

> 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 harbor" 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 laws to accommodate electronic discovery. For example, the Principles of *Sedona Canada*[59] are being applied across Canada in civil proceedings, and they have been incorporated by reference into the Ontario *Rules of Civil Procedure* — Rule 29.1.03(4).[60] There are

---

58 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)].

59 *The Sedona Canada Principles — Addressing Electronic Discovery*, online: The Sedona Conference, Canada, January 2008, *supra* note 4.

60 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

comparable rules of civil procedure in Canada's other jurisdictions.[61] And authoritative guidelines have been declared in various provinces.[62]

IX. "DUE DILIGENCE" IN REGARD TO THE PARTIES' RECORDS MANAGEMENT SYSTEMS

1. "Proportionality" doctrine and *Sedona Canada* apply to what the lawyers do in electronic discovery, but they do not apply to what the parties do in regard to the quality of their electronic records management. The parties have control of the records systems from which the records "discovered" come. Therefore potentially, they have more control over the adequacy and fairness of electronic discovery than do their lawyers. The word "parties" is used many times throughout *Sedona Canada*, but not in relation to the fundamental requirements of electronic records management or authoritative standards of electronic records management. The principles of proportionality are "records management dependent."[63] It follows that there should be a protocol of "due diligence" that the lawyers for the parties perform to provide some assurance in a formalized manner, that the records systems are capable of providing adequate and fair electronic discovery. Such is analogous to similar "due diligence" requirements imposed upon lawyers by other fields of law and legal practice. Such "due diligence" could be a series of questions based upon the national standard *72.34*, which is summarized in Appendix A herein.

2. Such "due diligence" may be answered by professional certification that the parties' record systems are in compliance with the National Standards of Canada for electronic records management, and in "legal compliance" with the major laws that depend upon electronic records and good records management. In place of such certification, could be the parties' affidavits (or the chief records officers' affidavits) that their records systems are in compliance with the national standards. Such affidavits would be subject to examination on discovery, and discovery by interrogatories.

3. Such "due diligence" is necessary because "proportionality" and *Sedona Canada* do not deal with the major and common defects of electronic records management systems that can significantly affect the quality of electronic discovery.

X. AMENDING THE *SEDONA CANADA PRINCIPLES* TO INCLUDE RECORDS MANAGEMENT

What follows are the Principles of *Sedona Canada* in published form, each followed by a suggested amended form of each principle, with Additional Com-

---

Discovery' developed by and available from The Sedona Conference. O. Reg. 438/08, s.25." (Operative from January 1, 2010).

61 See: "Appendix 1: Relevance and Proportionality in the Rules of Civil Procedure in Canadian Jurisdictions (August 2009)" in, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery*, *supra* note 4.

62 See the list of guidelines in, Ken Chasse, "The Admissibility of Electronic Business Records (2010), 8 Canadian Journal of Law and Technology 105 at 150, note 101.

63 But the principles are not written that way in, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery*, *supra* note 4.

ments, additional to those published. For Principles 3 and 9, no amendment is necessary, but "Additional Comments" are. The "amended principles" add their *italicized* words to those of the "published principles," along with a few differences in punctuation. And, "Additional Principle 1A" has been added. The most important and frequent difference is the absence of "the state of records management" as a relevant factor in every one of the *Sedona Canada Principles*.

"*Principle 1*: Electronically stored information is discoverable."

Amended Principle 1: Electronically stored information is discoverable, *but, because of differences in the state of electronic records management, not all electronic records management systems will be equally discoverable. Nonetheless, discovery of electronic records systems to produce electronic records and information should always be both fair and adequate*.

Additional Comment: Every principle, practice, and occurrence of electronic discovery is dependent upon the state of electronic records management, and is so dependent even when one ignores it or has no knowledge of it.

Additional Principle 1A: *Electronic discovery must not only be fair, but also adequate. The adequacy of electronic discovery requires that parties reveal the degree of compliance of their records systems with recognized standards of electronic records management. Such standards are based on the "system integrity" concept, i.e., the integrity of an electronic record is dependent upon the integrity of the electronic records system in which it is recorded or stored. Such "system discovery" is a necessary part of electronic discovery. Otherwise, compliance with the other Principles will be diminished and fairness to opposing parties will suffer*.

Additional Comment: Records management "system integrity" is a necessary part of: (1) the laws as to the admissibility of electronic records[64]; and, (2) the principles of electronic records management.[65] Therefore to make electronic discovery adequate, "system integrity" must be made a necessary part of the laws and principles of electronic discovery.

To have a workable definition of the "system integrity" concept of electronic records, plus explanatory guidance for its use, authoritative standards such as the National Standards of Canada for electronic records management must be applied. The national standards require that, "an organization shall always be prepared to produce its records as evidence."[66] To be able to do so adequately requires compliance with the requirements of "system integrity" as set out in those standards.

The nature of electronic records and the basic requirements of electronic records management made necessary by that very nature, constitute a technology that is the same everywhere that electronic records are recorded or stored. There-

---

64 Examples of the electronic record provisions in the Evidence Acts of Canada are cited in notes 2, 28, 46, and 56 and accompanying text *supra*, and they are listed in Appendix B *infra*. For comparable sections in the *Civil Code of Quebec* see note 56 *supra*.

65 The National Standards of Canada for electronic records management are; *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005; *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93, note 9 *supra*.

66 *Supra* note 9. See 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).

fore, in order to be sufficiently effective, the laws as to electronic discovery, admissibility, and the published principles of electronic records management must be compatible with that technology. For that reason, the laws of evidence concerning the admissibility of electronic records must incorporate as their foundation the "system integrity" concept. And laws of electronic discovery must be compliant with it.

In Canada, the "system integrity" concept is made part of the law of admissibility by those Evidence Acts having electronic records provisions,[67] and by the *Civil Code* of the province of Quebec.[68] The two provinces not yet having such provisions in their Evidence Acts will have to interpret the business record provisions as capable of applying the "system integrity" concept.[69]

Published principles and standards of electronic records management should define and elucidate the policies, practices, and rules of the "system integrity" concept. That is what the National Standards of Canada concerning electronic records management do.[70] They have been accepted by the Standards Council of Canada as national standards, and they have incorporated by reference, as "normative references," the standards of the International Organization for Standardization (the

---

67 The electronic records provisions for each jurisdiction in Canada are listed in Appendix B *infra*.

68 *Supra* note 56.

69 The two provinces, British Columbia and Newfoundland and Labrador, do not yet have electronic record provisions in their Evidence Acts. For British Columbia, its business record provision, (*Evidence Act*, R.S.B.C. 1996, c. 124, s. 42) will have to be interpreted so as to accommodate the "system integrity" concept. It uses the most commonly used "admissibility phrase" in such provisions in Canada, "a record made in the usual and ordinary course of business." The *Evidence Act* of Newfoundland and Labrador (*Evidence Act*, R.S.N.L. 1990, c. E-16), not having a business record provision, the common law business record exception to the hearsay rule will have to serve, its key phrase being, "a record of a regularly conducted activity." The comparable phase in (U.S.) Federal of Evidence 803(6), Public Law 93-595 § 1, Jan. 2, 1975 88 Stat.1926, is, "in the course of a regularly conducted business activity." But it also includes the words, "data compilation," which the Canadian business record provisions do not contain. "Data compilation" could be interpreted to incorporate the "system integrity" concept. Therefore FRE 803(6) can serve as a model for easily amending the Canadian business record provisions to an equivalent potential. Or, the definition of "record" used in the business record provision of Saskatchewan's *Evidence Act*, S.S. 2006, c. E-11.2, s. 50, might be copied. Its accompanying "definitions section," s. 49, provides this definition: "'record' includes any information that is recorded or stored by means of any device or electronic means." The words, "electronic means" may serve as well as "data compilation" to enable the "system integrity" concept to become an integral part of the interpretation and application of the business record provisions of all of the Evidence Acts. However, to be resolved would be the potential conflict between the subjective nature of the, "usual and ordinary course of business" phrase, and the objective nature of the "system integrity" concept, i.e., the former has no fixed definition other than that to be proved by evidence of the business activity of the "business" involved; but the latter looks to independent, authoritative standards of records management for definition of what records management "system integrity" should be.

70 *Supra* note 9.

ISO) concerning electronic technology, information technology, information processing, and data processing.[71] Therefore the "system integrity" concept provides a basis for declared principles of electronic records management common to all jurisdictions.

Such is the interdependent nature of admissibility, discovery, and the "system integrity" of records management. This "triangle of interdependence" should be made to operate in all jurisdictions. The nature of the technology of electronic records and of electronic records management dictates that it be made to be so.

"*Principle 2*: In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account (i) the nature and scope of the litigation, including the importance and complexity of the issues, interest and amounts at stake; (ii) the relevance of the available electronically stored information; (iii) its importance to the court's adjudication in a given case; and (iv) the costs, burden and delay that may be imposed on the parties to deal with electronically stored information."

Amended Principle 2: In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account (i) the nature and scope of the litigation, including the importance and complexity of the issues, interest and amounts at stake; (ii) the relevance of the available electronically stored information; (iii) its importance to the court's adjudication in a given case; (iv) the costs, burden and delay that may be imposed on the parties to deal with electronically stored information; *and, (v) that "proportionality" must not be defeated by inadequate electronic records management. The effects of inadequate records management upon the discovery process do not justify an argument that demands for disclosure and production are disproportionate*.

Additional Comment: The "proportionality" of electronic discovery is dependent upon the way in which electronically stored information is managed. The other four factors listed in this Principle are subject to the state of the electronic records management system(s) involved. "Bad" records management should not be an acceptable reason for designating a discovery request as "disproportionate." To maintain an equal application of procedural rules among the parties, the proportionality principle's "leveling processes" must impose sanctions for inadequate discovery caused by faulty records management.

"*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."

Amended Principle 3: [No amendment is necessary]

Additional Comment: What is a "reasonable step to preserve" depends upon how easy, costly, and effective preservation is. Inadequate records systems will render the preservation of electronically stored information arguably "unreasonable" in one way or another. Therefore the "proportionality" concept of Principle 2 should not be argued in defence of bad records management. Preservation should be an integral aspect of record system "retention-destruction" policies and practices.

"*Principle 4*: Counsel and parties should meet and confer as soon as practica-

71 *Supra* notes 9 and 41 and accompanying text.

ble, and on an ongoing basis, regarding the identification, preservation, collection, review and production of electronically stored information."

Amended Principle 4: Counsel and parties should meet and confer as soon as practicable, and on an ongoing basis, regarding the identification, preservation, collection, review and production of electronically stored information, *and regarding issues concerning the state of the electronic records management system(s) involved*.

Additional Comment: The cost, adequacy, timeliness, effectiveness, and fairness of all electronic discovery is dependent upon the state of the electronic records management systems producing the electronically stored information in question. Therefore, the degree of compliance of records systems with established and authoritative standards of electronic records management must be considered during the "meet and confer" sessions.

"*Principle 5*: The parties should be prepared to produce relevant electronically stored information that is reasonably accessible in terms of cost and burden."

Amended Principle 5: The parties should be prepared to produce relevant electronically stored information that is reasonably accessible in terms of cost and burden. *"Reasonably accessible" is not to be confounded by poor records management*.

Additional Comment: An electronic records management system that is very "non-compliant" with established principles of electronic records management can render all electronic discovery of electronically stored information very costly and burdensome. It can defeat electronic discovery's "proportionality" principle by making all information "unreasonably accessible." Therefore, allowance must be made for situations wherein one party has an excellent records management system and the other party has a terrible records management system, and for all situations in between those extremes.

"*Principle 6*: A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information."

Amended Principle 6: A party should not be required, absent agreement, *inadequate records management*, or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information.

Additional Comment: That which is "deleted or residual" depends upon the policies and practices one applies to one's records management of electronically stored information. Therefore a party should be accountable for its "deletions and residuals."

"*Principle 7*: A party may satisfy its obligation to preserve, collect, review and produce electronically stored information in good faith by using electronic tools and processes such as data sampling, searching or by using selection criteria to collect potentially relevant electronically stored information."

Amended Principle 7: A party may satisfy its obligation to preserve, collect, review and produce electronically stored information in good faith by using electronic tools and processes such as data sampling, searching, or by using selection criteria to collect potentially relevant electronically stored information. *However, where the state of a records management system is such that these tools and processes are ineffective so as to make electronic discovery inadequate, these obligations cannot be said to be satisfied. That fact must be disclosed to all other*

parties.

Additional Comment: [The following Additional Comment should be added to the second paragraph of Additional Comment 7.a. of the published Additional Commentary to Principle 7 of *Sedona Canada*. That paragraph states: "Although the benefits of using electronic tools and processes for data sampling, searching and review are obvious, especially when large volumes of electronic information are involved, these tools must be chosen with a view to their reliability, configured to ensure they operate properly, and used effectively by trained and experienced users. Ultimately, the reliability of the entire production process is dependent on the intelligent application of the appropriate tools. Any party who relies on technology (such as search engines to assist with the determination of relevance or privilege should submit that technology to a validation or audit process to ensure its efficacy."] Such validation or audit process should also include an assessment as to whether that technology can be effective in regard to the records management system(s) involved. Not only must "appropriate tools" fit and be compatible with the records system to which they are to be applied, but also that records system must be capable of being analyzed by those tools. The production process is dependent on the use of "appropriate tools," which in turn are dependent upon the state of electronic records management for their effectiveness.

"*Principle 8*: Parties should agree as early as possible in the litigation process on the format in which electronically stored information will be produced. Parties should also agree on the format, content and organization of information to be exchanged in any required list of documents as part of the discovery process."

Amended Principle 8: Parties should agree as early as possible in the litigation process on the format in which electronically stored information will be produced. Parties should also agree on the format, content and organization of information to be exchanged in any required list of documents as part of the discovery process. *Production can be affected by defects common to electronic records management systems. Parties should disclose to all other parties defects that affect the format, content, and organization of the electronically stored information to be produced.*

Additional Comment: Examples of relevant record system defects are: (1) if metadata is not preserved and tracked, it cannot be part of what is produced; (2) if there is no adequate classification or indexing system used to manage the records system, one will have to be created as part of what is produced; (3) a party has records systems that operate in accordance with conflicting principles and practices; (4) no audit trails or controls providing details as to deletions; (5) no "retention and disposal" program by which to track record lifecycles; and, (6) mergers and acquisitions producing unresolved conflicts in policy and procedure between records systems; and, (7) changes in records management technology used, unaccompanied by a proper "migration of electronic stored information" program producing "orphaned data," *i.e.*, records that can no longer be retrieved or read.[72]

"*Principle 9*: During the discovery process parties should agree to or, if necessary, seek judicial direction on measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronic documents and data."

---

72 A fuller list of such common defects is set out in section III above (p. 143).

Amended Principle 9: [No amendment is necessary.]

Additional Comment: Only by maintaining one's records system in compliance with the established, authoritative standards of electronic records management can one know sufficiently well what privileges, privacy, trade secrets and confidentialities one has to protect. Parties' and counsel's ability to perform this "duty of protection" is dependent upon the state of the records management system(s) involved. The worse the records system, the more judicial direction will be needed.

"*Principle 10*: During the discovery process, parties should anticipate and respect the rules of the forum in which the litigation takes place, while appreciating the impact any decisions may have in related actions in other forums."

Amended Principle 10: During the discovery process, parties should anticipate and respect the rules of the forum in which the litigation takes place, while appreciating the impact any decisions may have in related actions in other forums. *However, regardless the differences among the rules of multiple jurisdictions, to be adequate, it should be expected that electronic discovery in all jurisdictions will take account of the "system integrity" concept because of its compatibility with the nature of the technology that is electronic records and its records management*.

Additional Comment: Parties such as national and international organizations, have records systems in more than one jurisdiction. Jurisdictions have different laws of discovery and of evidence concerning the admissibility of electronic records, and possibly differences in their declared principles of electronic records management. The adequacy of discovery is not dependent on the law alone; it is dependent on and anchored in the nature of electronic records and what they make necessary for adequate electronic records management.

"*Principle 11*: Sanctions should be considered by the court where a party will be materially prejudiced by another party's failure to meet any obligation to preserve, collect, review or produce electronically stored information. The party in default may avoid sanctions if it demonstrates the failure was not intentional or reckless."

Amended Principle 11: Sanctions should be considered by the court where a party will be materially prejudiced by another party's failure to meet any obligation to preserve, collect, review or produce electronically stored information. The party in default may avoid sanctions if it demonstrates the failure was not intentional or reckless. *However, intentional, reckless, or otherwise inadequate records management that detracts from adequate electronic discovery does not provide a defence against sanctions. Records management not in compliance with accepted standards, such as the National Standards of Canada for electronic records management, is proof of inadequate records management*.

Additional Comment: The state of a party's electronic records management system is fixed before "litigation is contemplated." A party should not be heard to plead that state during the discovery process. The National Standards of Canada for electronic records management state: "An organization shall always be prepared to produce its records as evidence."[73]

"*Principle 12*: The reasonable costs of preserving, collecting and reviewing electronically stored information will generally be borne by the party producing it.

---

73 Notes 32 and 66 *supra* and accompanying texts.

In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order."

Amended Principle 12: The reasonable costs of preserving, collecting and reviewing electronically stored information will generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order. *However, a shifting of costs is not justifiable where a party's difficulty in making adequate and thrifty electronic discovery is due to its own faulty records management*.

Additional Comment: The largest costs of electronic discovery are generated by the state of electronic records management, and document review for relevance and privilege. "Bad" records management produces "bad" electronic discovery in every respect. All steps in the electronic discovery process are rendered to some degree cost-efficient or costly by that fact. The costs of document review can be reduced by: (1) complying with the "indexing" requirements of records management standards[74]; (2) using litigation support services; and, (3) using document review software. The cost of finding all relevant records can be reduced by strict compliance with recognized standards of records management.

After this article was submitted for publication, Lorman Education Services (*www.Lorman.com*) held an audio conference on July 6 and 27, 2011, entitled: *Fill it to the RIM: Best Practices in Drafting Records and Information Management Policies*. The description provided at this site states:

> Benefits
>
> As organizations are increasingly creating official records in electronic form, the 'data deluge' of high volumes of data has raised the importance of information management and the need for a comprehensive records and information management policy. The [U.S.] Federal Rules of Civil Procedure pertaining to e-discovery have heightened concerns regarding the obligation to preserve relevant documents, including electronically stored information (or ESI). Now, records and information management (RIM) is not only best practice but is also part of the minimum requirements for legal compliance. Organizations cannot keep everything. On the other hand, organizations cannot throw everything away. To reduce e-discovery and operating costs — and to avoid monetary and other sanctions — organizations need policies that enable them to effectively store, locate, retrieve and manage records.
>
> This live audio conference helps organizations understand how to get buy-in from key stakeholders and learn how to draft and implement a RIM Policy. The audio conference also explains the current best practices for records management and how to implement them in your program. The program addresses what should be included in the RIM policy and how to structure the policy for the most efficient implementation.

74 See for example section 6.5 (p. 23) of the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005, *supra* note 9.

Appendix A — A brief summary of electronic records management system compliance standards established by the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("72.34")[75]

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 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)].

---

75 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*, *supra* note 9. However, *72.11* is still the "industry standard" for the records management requirements of imaging.

4. The procedures manual and corporate records officer[76]: 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 corporate 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 prepared 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 pro-

76 *72.34* uses the term "corporate records officer" (CRO), instead of "chief records officer," or, "chief records manager, *supra* note 9." In section 3 of *72.34*, "Terms and definitions," is this definition (p. 6): "3.17 corporate records officer CRO, [the] organization Person authorized to act on behalf of the organization and entrusted for overall governance of the electronic record management program and related programs."

gram 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]

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 (electronic records); 30 (business records).

Alberta

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 (electronic records); (there is no business record provision).

British Columbia

Electronic Transactions Act, S.B.C. 2001, c. 10.

Evidence Act, R.S.B.C. 1996, c. 124, ss. 41.1–41.4 (electronic record court documents); s. 42 (business records).

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 (electronic records); 50 (business records).

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 (electronic records); 49 (business records).

Newfoundland and Labrador

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

Evidence Act, R.S.N.L. 1990, c. E-16 (has neither business record nor electronic record provisions).

Nova Scotia

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

Evidence Act, R.S.N.S. 1989, c. 154, ss. 23A to 23G (electronic records); 23 (business records).

Ontario

Electronic Commerce Act, 2000, S.O. 2000, c. 17.
Evidence Act, R.S.O. 1990, c. E.23, s. 34.1 (electronic records); 35 (business records).

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 (electronic records).
Evidence Act, R.S.P.E.I. 1988, c. E-11, s. 32 (business records).

Quebec

An Act to Establish a Legal Framework for Information Technology, R.S.Q. 2001, c. C1-1, ss. 2, 5–8, and 68 (electronic and business records).
Civil Code of Quebec, S.Q. 1991, c. 64, Articles. 2831–2842, 2859–2862, and 2869–2874 (electronic and business records).

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 (electronic records), 49-50 (business records).

Yukon

Electronic Commerce Act, R. S.Y. 2002, c. 66.
Electronic Evidence Act, R.S.Y. 2002, c. 67 (electronic records).
Evidence Act, R.S.Y. 2002, c. 78, s. 39 (business records).

Northwest Territories

Evidence Act, R.S.N.W.T. 1988. c. E-8, s. 37.1 (electronic records); s. 47 (business records).

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 (electronic records); s. 47 (business records).
Uniform Law Conference of Canada (the following are the "model Acts" for the above legislation):
Uniform Electronic Evidence Act (1998); online:
<http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2>
Uniform Electronic Commerce Act (1999); online:
<http://ulcc.ca/en/us/index.cfm?sec=1&sub=1u1>.

Appendix C

***Uniform Electronic Evidence Act* (UEEA)** As adopted by the Uniform Law Conference of Canada in 1998. The UEEA with commentary; online: <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2>. (the Model Act for the federal and provincial electronic evidence provisions in Canada)
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 Sub-sec 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.
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. [continued]
(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.
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)

Appendix D — *Uniform Electronic Commerce Act* (UECA) (the Model Act for the federal, provincial, and territorial electronic commerce Acts)

As adopted by the Uniform Law Conference of Canada (August 1999), online: <http://ulcc.ca/en/us/index.cfm?sec=1&sub=1u1>

Part 1 - Provision and Retention of Information

Part 2 - Communication of Electronic Documentsin

Part 3 - Carriage of Goods

1. Definitions — The definitions in this section apply in this Act.

(a) "electronic" includes created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means and "electronically" has a corresponding meaning.

(b) "electronic signature" means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document.

(c) "Government" means

(i) the Government of [enacting jurisdiction];

(ii) any department, agency or body of the Government of [enacting jurisdiction], [other than Crown Corporations incorporated by or under a law of [enacting jurisdiction]]; and

[(iii) any city, metropolitan authority, town, village, township, district or [rural municipality or other municipal body, however designated, incorporated or established by or under a law of [enacting jurisdiction].]

2. Application — (1) Subject to this section, this Act applies in respect of [enacting jurisdiction] law.

(2) The [appropriate authority] may, by [statutory instrument], specify provisions of or requirements under [enacting jurisdiction] law in respect of which this Act does not apply.

(3) This Act does not apply in respect of

(a) wills and their codicils;

(b) trusts created by wills or by codicils to wills;

(c) powers of attorney, to the extent that they are in respect of the financial affairs or personal care of an individual;

(d) documents that create or transfer interests in land and that require registration to be effective against third parties.

(4) Except for Part 3, this Act does not apply in respect of negotiable instruments, including negotiable documents of title.

(5) Nothing in this Act limits the operation of any provision of [enacting

jurisdiction] law that expressly authorizes, prohibits or regulates the use of electronic documents.

(6) The [appropriate authority] may, by [statutory instrument], amend subsection (3) to add any document or class of documents, or to remove any document or class of documents previously added under this subsection.

(7) For the purpose of subsection (5), the use of words and expressions like "in writing" and "signature" and other similar words and expressions does not by itself prohibit the use of electronic documents.

3. Crown — This Act binds the Crown.

4. Interpretation — The provisions of this Act relating to the satisfaction of a requirement of law apply whether the law creates an obligation or provides consequences for doing something or for not doing something.

PART 1 — PROVISION AND RETENTION OF INFORMATION

5. Legal recognition — Information shall not be denied legal effect or enforceability solely by reason that it is in electronic form.

6. Use not mandatory — (1) Nothing in this Act requires a person to use or accept information in electronic form, but a person's consent to do so may be inferred from the person's conduct.

(2) Despite subsection (1), the consent of the Government to accept information in electronic form may not be inferred by its conduct but must be expressed by communication accessible to the public or to those likely to communicate with it for particular purposes.

7. Requirement for information to be in writing — A requirement under [enacting jurisdiction] law that information be in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference.

8. Providing information in writing — (1) A requirement under [enacting jurisdiction] law for a person to provide information in writing to another person is satisfied by the provision of the information in an electronic document,

> (a) if the electronic document that is provided to the other person is accessible by the other person and capable of being retained by the other person so as to be usable for subsequent reference, and
>
> (b) where the information is to be provided to the Government, if
>
> > (i) the Government or the part of Government to which the information is to be provided has consented to accept electronic documents in satisfaction of the requirement; and
> >
> > (ii) the electronic document meets the information technology standards and acknowledgement rules, if any, established by the Government or part of Government, as the case may be.

9. Providing information in specific form — A requirement under [enacting jurisdiction] law for a person to provide information to another person in a

specified non-electronic form is satisfied by the provision of the information in an electronic document,

(a) *if* the information is provided in the same or substantially the same form and the electronic document is accessible by the other person and capable of being retained by the other person so as to be usable for subsequent reference, and

(b) where the information is to be provided to the Government, if

(i) the Government or the part of Government to which the information is to be provided has consented to accept electronic documents in satisfaction of the requirement; and

(ii) the electronic document meets the information technology standards and acknowledgement rules, if any, established by the Government or part of Government, as the case may be.

10. Signatures — (1) A requirement under [enacting jurisdiction] law for the signature of a person is satisfied by an electronic signature.

(2) For the purposes of subsection (1), the [authority responsible for the requirement] may make a regulation that,

(a) the electronic signature shall be reliable for the purpose of identifying the person, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made; and

(b) the association of the electronic signature with the relevant electronic document shall be reliable for the purpose for which the electronic document was made, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made.

(3) For the purposes of subsection (1), where the signature or signed document is to be provided to the Government, the requirement is satisfied only if

(a) the Government or the part of Government to which the information is to be provided has consented to accept electronic signatures; and

(b) the electronic document meets the information technology standards and requirements as to method and as to reliability of the signature, if any, established by the Government or part of Government, as the case may be.

11. Provision of originals — (1) A requirement under [enacting jurisdiction] law that requires a person to present or retain a document in original form is satisfied by the provision or retention of an electronic document if

(a) there exists a reliable assurance as to the integrity of the information contained in the electronic document from the time the document to be presented or retained was first made in itsfinal form, whether as a paper document or as an electronic document;

(b) where the document in original form is to be provided to a person, the electronic document that is provided to the person is accessible by the person and capable of being retained by the

person so as to be usable for subsequent reference; and

(c) where the document in original form is to be provided to the Government,

(i) the Government or the part of Government to which the information is to be provided has consented to accept electronic documents in satisfaction of the requirement; and

(ii) the electronic document meets the information technology standards and acknowledgement rules, if any, established by the Government or part of Government, as the case may be.

(2) For the purpose of paragraph (1)(a),

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display;

(b) the standard of reliability required shall be assessed in the light of the purpose for which the document was made and in the light of all the circumstances.

12. Whether document is capable of being retained — An electronic document is deemed not to be capable of being retained if the person providing the electronic document inhibits the printing or storage of the electronic document by the recipient.

13. Retention of documents — A requirement under [enacting jurisdiction] law to retain a document is satisfied by the retention of an electronic document if

(a) the electronic document is retained in the format in which it was made, sent or received, or in a format that does not materially change the information contained in the document that was originally made, sent or received;

(b) the information in the electronic document will be accessible so as to be usable for subsequent reference by any person who is entitled to have access to the document or who is authorized to require its production; and

(c) where the electronic document was sent or received, information, if any, that identifies the origin and destination of the electronic document and the date and time when it was sent or received is also retained.

14. Copies — Where a document may be submitted in electronic form, a requirement under a provision of [enacting jurisdiction] law for one or more copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single version of an electronic document.

15. Other requirements continue to apply — Nothing in this Part limits the operation of any requirement under [enacting jurisdiction] law for information to be posted or displayed in a specified manner or for any information or document to be transmitted by a specified method.

16. Authority to prescribe forms and manner of filing forms — (1) If a pro-

vision of [enacting jurisdiction] law requires a person to communicate information, the minister of the Crown responsible for the provision may prescribe electronic means to be used for the communication of the information and the use of those means satisfies that requirement.

(2) If a statute of [enacting jurisdiction] sets out a form, the [authority responsible for the form] may make an electronic form that is substantially the same as the form set out in the statute and the electronic form is to be considered as the form set out in the statute.

(3) A provision of [enacting jurisdiction] law that authorizes the prescription of a form or the manner of filing a form includes the authority to prescribe an electronic form or electronic means of filing the form, as the case may be.

(4) The definitions in this subsection apply in this section.

(a) "filing" includes all manner of submitting, regardless of how it is designated.

(b) "prescribe" includes all manner of issuing, making and establishing, regardless of how it is designated.

17. Collection, storage, etc. — (1) In the absence of an express provision in any [enacting jurisdiction] law that electronic means may not be used or that they must be used in specified ways, a minister of the Crown in right of [enacting jurisdiction] or an entity referred to in subparagraphs 1(c)(ii) [or (iii)] may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information.

(2) For the purpose of subsection (1), the use of words and expressions like "in writing" and "signature" and other similar words and expressions does not by itself constitute an express provision that electronic means may not be used.

18. Electronic payments — (1) A payment that is authorized or required to be made to the Government under [enacting jurisdiction] law may be made in electronic form in any manner specified by [the Receiver General] for the [enacting jurisdiction].

(2) A payment that is authorized or required to be made by the Government may be made in electronic form in any manner specified by the [Receiver General] for the [enacting jurisdiction].

PART 2 — COMMUNICATION OF ELECTRONIC DOCUMENTS

19. Definition of "electronic agent" — In this Part, "electronic agent" means a computer program or any electronic means used to initiate an action or to respond to electronic documents or actions in whole or in part without review by a natural person at the time of the response or action.

20. Formation and operation of contracts — (1) Unless the parties agree otherwise, an offer or the acceptance of an offer, or any other matter that is material to the formation or operation of a contract, may be expressed

(a) by means of an electronic document; or

(b) by an action in electronic form, including touching or clicking on an appropriately designated icon or place on a computer

screen or otherwise communicating electronically in a manner that is intended to express the offer, acceptance or other matter.

(2) A contract shall not be denied legal effect or enforceability solely by reason that an electronic document was used in its formation.

21. Involvement of electronic agents — A contract may be formed by the interaction of an electronic agent and a natural person or by the interaction of electronic agents.

22. Errors when dealing with electronic agents — An electronic document made by a natural person with the electronic agent of another person has no legal effect and is not enforceable if the natural person made a material error in the document and

(a) the electronic agent did not provide the natural person with an opportunity to prevent or correct the error;

(b) the natural person notifies the other person of the error as soon as practicable after the natural person learns of the error and indicates that he or she made an error in the electronic document;

(c) the natural person takes reasonable steps, including steps that conform to the other person's instructions to return the consideration received, if any, as a result of the error or, if instructed to do so, to destroy the consideration; and

(d) the natural person has not used or received any material benefit or value from the consideration, if any, received from the other person.

23. Time and place of sending and receipt electronic documents — (1) Unless the originator and the addressee agree otherwise, an electronic document is sent when it enters an information system outside the control of the originator or, if the originator and the addressee are in the same information system, when it becomes capable of being retrieved and processed by the addressee.

(2) An electronic document is presumed to be received by the addressee,

(a) when it enters an information system designated or used by the addressee for the purpose of receiving documents of the type sent and it is capable of being retrieved and processed by the addressee; or

(b) if the addressee has not designated or does not use an information system for the purpose of receiving documents of the type sent, when the addressee becomes aware of the electronic document in the addressee's information system and the electronic document is capable of being of being retrieved and processed by the addressee.

(3) Unless the originator and the addressee agree otherwise, an electronic document is deemed to be sent from the originator's place of business and is deemed to be received at the addressee's place of business.

(4) For the purposes of subsection (3)

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction to which the electronic document relates or, if there is no underlying transaction, the

principal place of business of the originator or the addressee; and

(b) if the originator or the addressee does not have a place of business, the references to "place of business" in subsection (3) are to be read as references to "habitual residence".

PART 3 — CARRIAGE OF GOODS

24. Actions related to contracts of carriage of goods — This Part applies to any action in connection with a contract of carriage of goods, including, but not limited to,

(a) furnishing the marks, number, quantity or weight of goods;

(b) stating or declaring the nature or value of goods;

(c) issuing a receipt for goods;

(d) confirming that goods have been loaded;

(e) giving instructions to a carrier of goods;

(f) claiming delivery of goods;

(g) authorizing release of goods;

(h) giving notice of loss of, or damage to, goods;

(i) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(j) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(k) notifying a person of terms and conditions of a contract of carriage of goods;

(l) giving a notice or statement in connection with the performance of a contract of carriage of goods; and

(m) acquiring or transferring rights and obligations under a contract of carriage of goods.

25. Documents — (1) Subject to subsection (2), a requirement under [enacting jurisdiction] law that an action referred to in any of paragraphs 24(a) to (m) be carried out in writing or by using a paper document is satisfied if the action is carried out by using one or more electronic documents.

(2) If a right is to be granted to or an obligation is to be acquired by one person and no other person and a provision of [enacting jurisdiction] law requires that, in order to do so, the right or obligation must be conveyed to that person by the transfer or use of a document in writing, that requirement is satisfied if the right or obligation is conveyed through the use of one or more electronic documents created by a method that gives reliable assurance that the right or obligation has become the right or obligation of that person and no other person.

(3) For the purposes of subsection (2), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(4) If one or more electronic documents are used to accomplish an action referred to in paragraph 24(j) or (m), no document in writing used to effect the action is valid unless the use of electronic documents has been terminated and replaced by the use of documents in writing. A document in writ-

ing issued in these circumstances must contain a statement of the termination, and the replacement of the electronic documents by documents in writing does not affect the rights or obligations of the parties involved.

(5) If a rule of [enacting jurisdiction] law is compulsorily applicable to a contract of carriage of goods that is set out in, or is evidenced by, a document in writing, that rule shall not be inapplicable to a contract of carriage of goods that is evidenced by one or more electronic documents by reason of the fact that the contract is evidenced by electronic documents instead of by a document in writing.