# "Records Management Law"—a Necessary Major Field of the Practice of Law

*Ken Chasse*[*]

## INTRODUCTION

"Records management law" will be a necessary area of specialization because: (1) electronic records are now produced by most commercial, communication, transmission of data, and social, formal, and semi-formal interactions; (2) therefore they are the foundation of many kinds of legislation; (3) records are the most frequently used kind of evidence in legal proceedings; and, (4) electronic records are as important to daily living as are motor vehicles, and will become more important. But the legal infrastructure of statutes, guidelines, and case law that controls the use of electronic records as evidence is very inadequate because it ignores these facts: (1) electronic records technology and pre-electronic paper records technology are very different technologies—each requires its own legal infrastructure; (2) there are many serious defects frequently found in electronic records management systems (ERMSs), and in their software; (3) there is an electronic records "system integrity" concept that has to be in the evidence laws; (4) the national and international standards for electronic records management need to provide definitions and the principles of ERMS practice necessary for the effective operation of that concept; and (5) the solution to the high cost of the "review" stage of electronic discovery proceedings requires a different strategy and procedure than what are used now. Because of these shortcomings and society's heavy dependence upon electronic records, "records management law" is a needed specialty, and the "records management lawyer" a needed specialist. The several innovations, concepts, and arguments developed in this article have been made possible by what I have learned from working with experts in electronic records management for many years. Such innovations are needed to make all litigation available at a reasonable cost.

---

[*] Ken Chasse J.D., LL.M., member of the Law Society of Upper Canada (province of Ontario), and of the Law Society of British Columbia, Canada. SSRN author's page: <http://ssrn.com/author=1398484>, and Slaw blog author's page: <http://www.slaw.ca/author/chasse/>.

## I. THE SERIOUS DEFECTS CAUSED BY THE INADEQUATE LEGAL INFRASTRUCTURE CONTROLLING THE USE OF ELECTRONIC RECORDS AS EVIDENCE[1]

Working with experts in electronic records management systems technology (ERMS technology) since 1978 has taught me the substantial consequences of the fact that an electronic record, *unlike* a pre-electronic paper record, is dependent upon its ERMS for everything, including its existence, its accessibility, and its integrity. Therefore, the laws and practices controlling electronic discovery and admissibility of evidence proceedings are very inadequate because they take no account of these serious defects very frequently found in ERMSs:

- the extent of the records holdings is unknown;
- records are neither properly classified nor indexed, such that retrieval of relevant records is very difficult if not impossible;
- no definitive classification system exists among institutional, transitory, and personal records;
- there is either no records manual, or one that isn't kept current or complied with;
- there are no bylaws (or orders of comparable authority from senior management) dealing with the records system, which is essential for establishing an organization's "usual and ordinary course of business" in regard to its records system;[2]
- email is not classified, indexed, or pruned, or possibly not retained; there is no "email protocol" operative throughout the organization;
- records repositories are not well defined nor centrally accessible;
- there is 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

---

1 Many times have I reviewed the reports of experts in electronic records technology as to the state of their clients' records managements systems. They are the basis of my legal opinions as to the ability of those systems to comply with the laws and the National Standards of Canada for electronic records management; *infra* note 7.

2 That phrase is the business record admissibility rule in the Evidence Acts of 12 of Canada's 14 jurisdictions (10 provinces, 3 territories, and the federal jurisdiction); *e.g.*, s 30(1) of the *Canada Evidence Act*, RSC 1985, c C-5 [CEA]; s 35 of the (Ontario) *Evidence Act*, RSO 1990 c E.23; and s 42 of the British Columbia *Evidence Act*, RSBC 1996, c 124. The Evidence Acts of Alberta and Newfoundland and Labrador do not contain such provisions. The same phrase is used in the electronic records provisions of 11 of the Evidence Acts as a presumption of "integrity": *e.g.*, s 31.3 of the *Canada Evidence Act*; s 34.1(7)(c) of the Ontario *Evidence Act*; and, s 41.5(c) of the Alberta *Evidence Act*, RSA 2000, c A-18. Comparable phrases are used in the *Civil Code* of Québec, LRQ, c C-1991, Book 7, and in An Act to Establish a Legal Framework for Information Technology, CQLR c. C-1.1. Only the Evidence Acts of British Columbia, Newfoundland and Labrador, and of the Northwest Territories do not contain electronic records provisions.

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 there are extensive duplicates and an inability to track official or original versions;
- there are no audit trails or controls detailing deletions, *i.e.*, when, who, or by what retention/destruction/disposal authority;
- there is no clear definition or practice as to what is the "deletion" of a record such that 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 have resulted in unaccounted for and undocumented changes in records practice;
- there is no consistent practice as to other forms of communication that create records, *e.g.*, video and audio recordings, instant messaging, and cellphone (mobile) communications;
- there is 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 exists;[3]
- there is "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);
- there is poor security[4] protection; [5]

---

[3] The National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("*72.34*"), *infra* note 7 and accompanying text, uses the term, "Corporate records officer (CRO)," (definition at p. 6, term number 3.17).

[4] The ninth in the list of points in proof of "system integrity," (*infra* note 20) specified in the National Standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 (*infra* note 7) 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;

- there is inadequate compliance with the records management requirements of the privacy laws;[6]
- there exists inadequate testing, auditing, and quality control; and
- there is substantial non-compliance with the National Standards of Canada concerning records management, and a lack of appreciation of the consequences of non-compliance.[7]

---

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].

5 The article, "Practice Tips for Mitigating Data-Breach Risk and Liability," by Michael T McGinley (2 April 2014) *Litigation-Criminal Litigation* (website) online: American Bar Association < http://goo.gl/FUEJ53 > , states in part: "In 2013, reported data breaches reached an all-time high—at least 740 million records were compromised. Press Release, Online Trust Alliance (OTA), Online Trust Alliance Finds Data Breaches Spiked to Record Level in 2013; 89 Percent Could Have Been Prevented (Jan. 22, 2014). Businesses understandably are concerned because these breaches can be enormously costly. In 2012, for example, the average total organizational cost of a data breach to a U.S. company was over $5.4 million. . . . The recent data breach at Target Corp. offers a stark example: Some analysts estimate that Target's breach may end up costing the company close to $1 billion. Smaller firms fare no better against breaches and have less ability to absorb losses. The cyber-security forecast for U.S. businesses is dark". See, John Vomhof Jr, "Target's data breach fraud cost could top $1 billion, analyst says", online: (2014) Minneapolis/St. Paul, Business Journal < http://goo.gl/wE3ezK > .

6 For example, s 5 in Part 1,"Protection of Personal Information in the Private Sector," of the *Personal Information Protection and Electronic Documents Act*, SC 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 PIPEDA, applies federally and 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 (with counterparts in the 13 other jurisdictions). Part 3, "Amendments to the Canada Evidence Act," added the electronic records provisions to the *CEA*, ss 31.1-31.8 (with counterparts in the other jurisdictions, except British Columbia, Newfoundland and Labrador, and the Northwest Territories).

7 The National Standards of Canada are: (1) *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005 ("*72.34*"), published in 2005; and, (2) *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93 ("*72.11,*" updated to 2000; first published in 1979 as, *Microfilm as Documentary Evidence*). *72.34* incorporates all that *72.11* deals with but *72.11* has remained the ERMS industry standard for "imaging" procedures, *i.e.*, the large industry for converting original paper records to digital storage. The electronic records provisions were enacted to enable all digitally stored records to be accepted as original records. These standards were developed by the CGSB

These defects are frequently found in the ERMSs of all organizations. The reasons why they are very common are: (1) there is no law of general application requiring ERMSs be maintained in compliance with any standard, such as the National Standards of Canada for electronic records management; and (2) many organizations find that they can "get along just fine" using only their most recently made and received records. In litigation it is the older records, however, that are equally important in interpreting the meaning of a contract or other event that occurred at the time when those older records were made. Many of the records often used as evidence were created or received when a very different kind and quality of records management was operative. Therefore, there can be no assurance that all relevant records have been disclosed, or that those disclosed are still in the form in which they were created. It is necessary to ask, "are they in their original form, or corrupted or contrived copies?"

Electronic discovery and admissibility proceedings should be able to be used to reveal such serious defects, but their existence is ignored. Various pieces of an ERMS are demanded, such as records, metadata, email, and designated storage devices, but there is no demand for proof of records management reliability and "integrity" (being the word used in the electronic records provisions that are in 11 of the 14 Evidence Acts in Canada).[8] Electronic discovery is conducted without a records management audit or comparable certification of records management quality. Proof of the existence of the defects listed above could result in: (1) establishing the probability that relevant records are not available; (2) inadequate disclosure and discovery of records; and, (3) the inadmissibility of records as evidence, or the absence of the necessary "weight" that gives records the appearance of having sufficient reliability.

The law as applied does not require proof of records management quality. It is a law written on the unchallenged assumption that electronic records, and their ERMS technology, are just a faster and more convenient version of pre-electronic paper records management technology—like adding a motor to a bicycle, instead of replacing the bicycle with a motor vehicle—and soon, electronic technology's need for a legal infrastructure will be as complex as that governing airplanes. In fact, they are very different technologies, requiring very different laws that regulate and enforce their use. As a result, electronic discovery and admissibility proceedings enable the use of records as evidence that have an

---

(Canadian General Standards Board), a standards-writing agency within Public Works and Government Services Canada. CGSB is accredited by the Standards Council of Canada as a standards-development agency. Certification as a National Standard of Canada by the Council requires compliance with designated procedures—see its "operations" of the Standards Council of Canada (webpage) online: < http://www.scc.ca/en/about-scc/operations > . *72.34* incorporates as "normative references," many of the standards of the International Organization for Standardization ("ISO," an acronym for all languages), in Geneva, Switzerland. A CGSB committee is now updating these standards. I have acted as a legal advisor in the creation of both standards and updating them.

8 *Supra* note 2.

unacceptably high probability of being unreliable and otherwise inadequate. That information, however, would not be known at the time when courts make decisions based upon such records.

The distance between discovery's and admissibility's simplicity and reality's complexity is aggravated by the fact that organizations are moving away from centralized ERMSs. Records systems are becoming a network of applications existing in-house, in mobile devices, and in centralized, shared utility services such as "the cloud." Records do not sit in a single records management system. They constantly move among systems; transmission creating a "weak link" as to proving integrity. Therefore, rather than focusing on in-house ERMSs, laws and records management standards will have to focus on records management, and on the amount of control embedded in records management policies, procedures, and processes. Going from paper to electronic records will require as much change in our legal infrastructure as going from horses to motor vehicles.

## II. SOFTWARE ERRORS AND VULNERABILITIES ARE VERY PREVALENT AND COSTLY

In addition to the prevalence of such serious, ignored errors are the numerous errors in the software that all ERMSs depend upon. Many ERMSs operate on several million lines of software code, and it has an error rate as do most things created by people. For example, the Windows 3.1 operating system has close to 3 million lines of software code. The Google Chrome web browser has approximately 5 million lines. The Firefox browser is near 10 million, and Windows 7 has under 40 million lines of code, which is a little less than Windows XP, and more than 10 million less than Windows Vista. An Android phone has more than 12 million lines of code. As a result, "Updates" also contain software error corrections. In 2002, a study commissioned by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) concluded that, "software errors cost the U.S. economy $59.5 billion annually."[9] Their report states, in part:

> "The impact of software errors is enormous because virtually every business in the United States now depends on software for the development, production, distribution, and after-sales support of products and services," said NIST Director Arden Bement. "Innovations in fields ranging from robotic manufacturing to nanotechnology and human genetics research have been enabled by low-cost computational and control capabilities supplied by computers and software."
> In 2000, total sales of software reached approximately $180 billion, supported by a large workforce encompassing 697,000 software engineers and 585,000 computer programmers.

---

[9] NIST, NIST Planning Report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing* (May 2002) online: <http://web.archive.org/web/20090610052743/http:/www.nist.gov/public_affairs/releases/n02-10.htm>.

> Software is error-ridden in part because of its growing complexity. The size of software products is no longer measured in thousands of lines of code, but in millions. Software developers already spend approximately 80 percent of development costs on identifying and correcting defects, and yet few products of any type other than software are shipped with such high levels of errors. Other factors contributing to quality problems include marketing strategies, limited liability by software vendors, and decreasing returns on testing and debugging, according to the study. At the core of these issues is difficulty in defining and measuring software quality.
>
> The increasing complexity of software, along with a decreasing average product life expectancy, has increased the economic costs of errors. The catastrophic impacts of some failures are well-known. For example, a software failure interrupted the New York Mercantile Exchange and telephone service to several East Coast cities in February 1998. But high-profile incidents are only the tip of a pervasive pattern that software developers and users agree is causing substantial economic losses.[10]

Therefore, the untested "assumption of reliability and regularity" that the legal community applies to the use of devices dependent upon software is unjustified and dangerous.[11] All devices, electronic or otherwise, must be assumed to be prone to error such that the evidence they provide should not be accepted as reliable unless there is expert opinion evidence or some other form of authoritative certification of their reliability.

An example of unexpected unreliability in a much used and "faithful" electronic device is provided in this recent news story: "Xerox scanners/photocopiers randomly alter numbers in scanned documents."[12] Also of concern is the current frequency of "hacking" into everything electronic, for example, this article: "Why Apple's Recent Security Flaw is Scary."[13]

The software in breathalyzer-type machines, which one would assume would have to be more reliable than that in most other electronic devices, nonetheless has a significant error rate. The following quotation uses the term "source

---

[10] *Ibid.*

[11] See Stephen Mason, ed, *Electronic Evidence*, 3rd ed., (LexisNexis Butterworths, 2012), chapter 5; "Electronic evidence: A proposal to reform the presumption of reliability and hearsay" (2014) 40 *Computer Law and Security Review* 1, 80 — 84; *Mason Report of the IALS Think Tank* on the reform of the law concerning the presumption that mechanical instruments—in particular computers (now an out-of-date concept)—are "in order," online: < http://ials.sas.ac.uk/news/IALS_Think_Tank.htm > .

[12] David Krisel, "Xerox scanners/photocopiers randomly alter numbers in scanned documents" (2 August 2013) online: < http://goo.gl/PJZNNp > . The text of this article is somewhat informal in places but nonetheless persuasive.

[13] Brian Barrett, "Why Apple's Recent Security Flaw is so Scary" (23 February 2014) online: Gizmodo < http://gizmodo.com/why-apples-huge-security-flaw-is-so-scary-1529041062 > .

code"[14] in reference to the software in a particular make and model of breathalyzer machine:[15]

> . . . . On average, 25 software defects exist for every 1,000 lines of code. If the number of lines of code in the source code can be ascertained, the industry averages can be applied to estimate the number of defects. The estimated number of defects is calculated by multiplying the number of lines of code by 25, and dividing that product by 1,000.
> The number of lines in the source code has been disclosed in testimony for the Draeger 7110 device, which has 53,774 lines of code that print out on 896 pages. Applying the formula that utilizes the industry average, it is reasonable to expect 1,344 defects in the software for the Draeger 7110, if it conforms to the industry norms and is "average".

The ability to detect the implanting of malicious software is very poor. The following quotation is from an article dealing with the "Trojan horse defence", *i.e.*, defences against accusations of illegal materials found in a computer that claim that a malicious program, hidden within a properly obtained program, was the cause of the implanting:[16]

> Daniel Bilar explains how antivirus programs work, and points out that a lot of malicious codes are not recognized by antivirus software that is not updated regularly. Between 26 and 31 per cent of malicious software is not detected on antivirus programs that are not up-dated for a week (this percentage is only valid for better antivirus programs — poor quality antivirus programs can miss up to 80 per cent of malicious codes). It is clear that it is reasonably probable, and not only a hypothetical exception, that a computer can be infected with a Trojan horse. It is important to be aware that although people might have a basic understanding of technology (for instance, the majority will not necessarily open strange files received by e-mail), very few are aware of the fact that they can download various forms of malicious code (such as Trojan horses) simply by launching an URL site, opening a PDF document or browsing internet pages. Up-dated antivirus software,

---

[14] "Source code" contains programming techniques and is essential documentation recording the development of software. To evaluate software, one needs its source code. See Wikipedia online: < http://en.wikipedia.org/wiki/Source_code > .

[15] This quotation comes from page 14 of the following article, dealing with the considerable volume of litigation challenging the source code of Intoxilyzer, Breathalyzer, and Alcotest machines and their operation: William C Head and Thomas E Workman Jr, "An Analysis of "Source Code" in the United States: What Challenges Have Been Asserted, and Where is this Litigation Heading Analysis of 'Source Code'?" presented at the *International Council on Alcohol, Drugs and Traffic Safety*, Seattle Washington, 30 August 2007. See also, Charles Short, "Note: Guilty by Machine: The Problem of Source Code Discovery in Florida DUI Prosecutions," (2009) 61 Fla L Rev 177 . DUI = driving under the influence (of alcohol or drugs).

[16] Miha Sepec, "The Trojan Horse Defence—A Modern Problem of Digital Evidence" (2012) 9 Digital Evidence and Electronic Signature Law Review 58 at 61, online: < http://journals.sas.ac.uk/deeslr/article/view/1990 > .

> firewalls, and caution on the internet help reduce the risk, but cannot completely eliminate it.
>
> . . .
>
> Testing of malware developed for the purposes of stealing personal information and account credentials has revealed that, on average, 60% are not detectable by anti-virus software at the time they are discovered in the wild. Therefore, client computers with the most "up to date" anti-virus software signatures are likely to be vulnerable to such attacks about 60% of the time. [footnotes omitted]

Therefore, on an application for production of the specifications and testing of an electronic device or of an ERMS, should one have to specify exactly what the defects are and what their effects will be? The answer should be "no." Statements such as those above can be authoritatively supported with evidence as to the potentially serious negative effects of such software defects. However, if the software has been authoritatively certified as being reliable and producing accurate results,[17] then such statements alone should not be sufficient to justify a production order for further evidence or witnesses for cross-examination. One would have to attack the certification process, or the particular device used in one's case, or its operation.[18]

This exemplifies the importance of authoritative standards such as Canada's national standards for electronic records management.[19] Dangerous is the legislating of a "cutting costs by cutting competence" presumption of regularity, so as to make legal proceedings cost less and take less time by forcing the acceptance of the evidence produced by such electronic devices and systems. Such a presumption casts a burden of proof on the opposing party to provide "evidence to the contrary" that the evidence produced by the device is unreliable. To the contrary, the law should require proof of compliance with such standards as a condition-precedent to having such evidence accepted as reliable. The rebuttable presumption to be legislated would state that without proof by certification or other sufficient evidence of such compliance with authoritative standards of performance, the evidence produced by the electronic device or system in question is presumed to be unreliable. Such presumption puts the onus of proof where it should be—on the party that uses the device or system to produce the evidence in question.

---

[17] For example, breathalyzer-type instruments used in relation to impaired driving and "over 80" (DUI) prosecutions under Canada's *Criminal Code*, RSC 1985 c C-46, ss 253(1)(a),(b), 258, are officially approved for use by way of the Approved Breath Analysis Instruments Order, SI/85-201. This Order approves certain analysis instruments as being suitable for the purposes of s 258 of the *Criminal Code*. See also ss 254 and 254.1.

[18] For example, attacking the operation of, and the results provided by, a breathalyzer-type instrument is provided for by s. 258(1)(c) of the *Criminal Code*, *supra* note 17.

[19] *Supra* note 7.

## III. THE THREE ANALOGIES THAT EXEMPLIFY THE NECESSARY CONCEPTUAL FOUNDATION FOR AN ADEQUATE LAW

The following three analogies should be the foundational concepts for all that is written and done in regard to the discovery and admissibility of electronic records:

### (a) The Drop of Water Analogy

An electronic record is merely an electronic impression upon an electronic storage device, which is but a part of an electronic records management system (an ERMS). An electronic record in its ERMS is like a drop of water in a pool of water. Like a drop of water, an electronic record is dependent upon its ERMS (its "pool") for its: (a) existence; (b) accessibility; and (c) its integrity—records integrity depends upon records system integrity. That is the "system integrity" concept.[20] But a pre-electronic paper record is not dependent upon its records system for any of those three factors. Its medium of storage is paper or microfilm, and not a complex electronic storage device, such as a hard drive, which is most often just one small part of a large, complex ERMS. Paper and microfilm are very simple storage media, rarely requiring proof of their ability to serve as storage media. But electronic devices and ERMSs are complex storage media of infinite variety, purpose, and quality of maintenance, dependent upon the reliability of millions of lines of software code. An electronic record can be a record without having to be constantly in readable, reviewable form, and without having to be on a physical, tangible medium of storage such as paper or microfilm. In contrast, the contents of a pre-electronic record cannot be a record without being on a physical, tangible medium of storage such as paper or microfilm.

These differences mean that electronic records technology and pre-electronic paper records technology are very different technologies, needing very different bodies of law regulating their use. Therefore, the laws and practices as to discovery and admissibility of evidence must be different for electronic records than they are for pre-electronic paper records. So far, the Canadian statutory law of admissibility is different in 11 of Canada's 14 jurisdictions (10 provinces, 3 territories, and the federal jurisdiction), but it has not changed the evidence adduced and procedures used in admissibility proceedings, and the law and practice controlling electronic discovery show no recognition of the differences between electronic records technology and paper records technology. That is

---

[20] Within the electronic records provisions of the Evidence Acts that contain such provisions (*supra* notes 2 and 6, and the "system integrity concept," below). Because all laws concerning the use of electronic records as evidence are based upon ERMS technology, the "system integrity concept" is relevant to all such proceedings, regardless whether the applicable Evidence Act contains such provisions. Laws based upon the use of any technology that ignore the weaknesses and dangers of that technology create an unacceptability high probability of inaccurate and unjust results.

because the understanding of what a record is has not changed. An electronic record is viewed as being of the same nature as a pre-electronic paper record, but merely much easier and convenient to create, store, and transmit. That is why ERMSs are not considered in the case law, and that is why the legal infrastructure concerning electronic discovery and admissibility is inadequate, and therefore at substantial risk of producing decisions that are inaccurate and unfair.[21]

### (b) The Expert Witness's Qualifications Analogy

Using an electronic record for any "legal" purpose without inquiring into the quality of electronic records management of the ERMS in which the record is stored is like using an expert witness without inquiring into the qualifications of that expert. Without such qualifications, the worth of the expert's evidence cannot be assessed. Such use of expert evidence would be negligence. Similarly, the worth of the evidence provided by an electronic record cannot be assessed without evidence as to the state of records management of the ERMS in which the electronic record is stored. Its "qualifications" are those of its ERMS. Therefore, law and practice should move quickly to the day when use of an electronic record for any purpose having legal consequences, without regard to the quality of the records management of the ERMS in which it is stored, should also be considered an act of negligence. If an ERMS is small, such concern might not need a records management expert, but should not escape the need for proof of quality.

### (c) The Horses to Motor Vehicles Analogy

Stepping up to a new technology requires that it be controlled by new laws and regulations, otherwise it will cause injury, damage, and unfairness. For example, going from a horse-powered transportation system to a motor-vehicle-

---

[21] For example, the decision in *Zenex Enterprises Ltd. v. Pioneer Balloon Canada Ltd.*, 2012 ONSC 7243, 2012 CarswellOnt 15976, [2012] O.J. No. 6082 (Ont. S.C.J.) in effect holds that the state of a party's electronic records management system (ERMS) is irrelevant to electronic discovery proceedings. Specifically, it holds (para 8) that the parties are not to demand to know how searches for relevant records were conducted, nor can they investigate parts of an opposing party's ERMS, such as hard drives. This ignores the fact that the accessibility and storage of electronic records are essential parts of ERMS technology. Electronic discovery cannot produce fair and accurate results unless the quality of the parties' electronic records management is investigated, particularly so its compliance with the National Standards of Canada for electronic records management, *Electronic Records as Documentary Evidence*, CAN/CGSB-72.34-2005 (*supra* note 7). See also: *Warman v. National Post Co.*, 2010 ONSC 3670, 2010 CarswellOnt 5920, 103 O.R. (3d) 174, [2010] O.J. No. 3455 (Ont. Master), additional reasons 2010 CarswellOnt 11136 (Ont. Master), specific directions given at paras 166-181; *Direct Energy Marketing Ltd. v. National Energy Corp.*, 2013 ONSC 4048, 2013 CarswellOnt 13871, [2013] O.J. No. 4533 (Ont. S.C.J.); and *1483860 Ontario Inc. v. Beaudoin*, 2010 ONSC 6294, 2010 CarswellOnt 9424, [2010] O.J. No. 5315 (Ont. Master), reversed in part 2011 CarswellOnt 12513 (Ont. S.C.J.).

based transportation system has required a vast amount of new laws, regulations, and enforcement personnel, including police officers, judges, and lawyers. Without all of that additional "legal infrastructure," motor vehicle transportation would be too dangerous to use. Similarly, going from pre-electronic paper records and paper-based records management systems to our present electronic records and ERMSs is stepping up to a new technology that is in the process of causing changes that will be just as great and far-reaching as motor vehicles, and eventually more so; however, the present legal infrastructure for this new technology is inadequate. Therefore, decisions in regard to electronic discovery, admissibility, electronic commerce, and communications will often be wrong and unfair. Unfortunately, the probability of those negative consequences happening, being consequences to be prevented by "doing justice," will not be known nor adequately assessed at the time of decision-making.

## IV. THE NECESSARY PRINCIPLES FOR THE USE OF ELECTRONIC RECORDS AS EVIDENCE

Those three concepts give rise to the following principles. They must be made to interact compatibly, or there will not be an adequate records management and legal infrastructure regulating the use of electronic records in legal proceedings. To implement and maintain this infrastructure, "records management law" is a needed specialty.

> Documentary Discovery (before trial), "Every document relevant to any matter in issue in an action that is or has been in the possession, control or power of a party to the action shall be disclosed. . . ," being Rule 30.02(1) of the province of Ontario Rules of Civil Procedure.[22]
>
> "Proportionality": "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." Principle 2 of *The Sedona Canada Principles—Addressing Electronic Discovery*.[23]
>
> "The prime directive": "an organization shall always be prepared to produce its records as evidence" (from the National Standard of Canada, Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005 [hereinafter, "*72.34*"], subsection 5.4.3(c) at p. 17).[24] This principle is essential to the enforcement of the principles defining the

---

[22] RRO 1990, Reg 194.

[23] The four *Sedona Canada* texts concerning electronic discovery are listed in note 32, *infra*. See also section V below, "Guidelines for electronic discovery proceedings." It deals with the inadequacy of the *Sedona Canada Principles—Addressing Electronic Discovery* text.

[24] *Supra* note 7.

function of the needed "records management law" practice group of lawyers. The next three statements provide the conceptual foundation of "records management law."

The "system integrity concept": records integrity requires proof of records system integrity—s. 31.2(1)(a) of the *Canada Evidence Act*, and comparable provisions in the electronic records provisions of the other Evidence Acts in Canada.

The "triangle of interdependent concepts" for the use of electronic records as evidence: (1) the "system integrity concept" (of the electronic records provisions of the Evidence Acts);[25] (2) the "prime directive" (of *72.34*, the National Standard of Canada for ERMSs);[26] and, (3) the "proportionality principle" (of all guidelines concerning the procedures for electronic discovery proceedings).[27] Compliance with the "prime directive" would: (1) greatly facilitate applying the "system integrity concept" in electronic discovery and admissibility of evidence proceedings; and (2) the "proportionality principle" would not allow undisclosed bad records management to be used as the basis for an argument of "disproportionality" so as to escape demands for further disclosure of relevant records. "Proportionality" would thus in turn provide further support to the other two concepts. The interdependent nature of the concepts of this "triangle" is thus made complete. The efficacy of electronic discovery and admissibility proceedings is dependent upon the effectiveness of these relationships, which in turn are dependent upon compliance with authoritative standards of electronic records management.

The "triangle of interdependent proceedings": (1) electronic discovery proceedings; (2) admissibility proceedings concerning electronic records as evidence; and (3) proof of compliance with authoritative standards for ERMS technology (such as Canada's National Standards), by the ERMSs that produce the records used as evidence. One of the purposes of all discovery proceedings is to reveal what records there are available as potentially admissible evidence. But now, ERMS technology makes necessary an additional purpose—to provide the records management information of the "discovered" records that is relevant to the requirements of admissibility. One cannot know if an electronic record is admissible unless one knows whether the record can satisfy the concepts within the "triangle of interdependent concepts." Discovery proceedings that do not provide such information about disclosed records create an unacceptably high probability of inadequate records being used as evidence.

Criminal as well as civil proceedings: The issues and problems dealt with below are now seriously plaguing civil proceedings. Therefore, the solutions provided are aimed at those civil litigation problems;

---

[25] *Supra* note 20, and below: Section VII, The System Integrity Concept at p. 89.

[26] *Supra* note 7.

[27] The chief guideline in the *Sedona Canada Principles-Addressing Electronic Discovery*, *infra* note 32.

> however, almost all that is stated herein is applicable to criminal proceedings. The broad duty of disclosure imposed upon the Crown prosecutor by the Supreme Court of Canada in *R. v. Stinchcombe*,[28] and its case law and other analytical progeny, does not alter the fact that the "system integrity concept" that is the foundation of the electronic records provisions of sections 31.1 to 31.8 of the *Canada Evidence Act* (ss. 31.1-31.8), and of ERMS technology, is applicable and operative in all legal proceedings involving the use of electronic records. To fulfill its purpose, a law based upon a technology cannot ignore the dangers and requirements of that technology. Therefore the "*Stinchcombe* duty of disclosure" should include information as to the state of records management of the ERMSs from which the records disclosed were obtained, and at the time they were made or received, and also at the time they were disclosed so comparisons can be made. For example, what was the state of compliance of those ERMS's with the national standards for records management at those times? That asks, in effect, how probable is it that the defects in the list set out at the beginning of this article were operative at those times?[29]

Such information may not be possible to obtain because: (1) records systems are constantly changing as indicated in that list of defects; and (2) records are often obtained by the police long before charges are laid, and disclosure is most often made even further beyond the time of obtaining the records. The state of records management at the time of disclosure is often not the same as at those earlier times. The ability to obtain all relevant records, with the "integrity" required by the electronic records provisions of the Evidence Acts, depends upon the time when the records were made or received, and at the time when the searching for them was done. Police practice does not include providing information as to the state of records management. Therefore, in cases dependent upon records as evidence, the accused person's right to "a fair trial" (*Canadian Charter of Rights and Freedoms* s. 11(d)) and "full answer and defence" (s. 7 "fundamental justice"), might be in jeopardy.[30] If records systems were kept constantly in compliance with Canada's national standards, or at the least with international standards for electronic records management (if accepted as substitutes), none of these issues would arise.

Keeping ERMSs in compliance with established standards so that laws may assume the reliability of the records they produce is just as important as keeping

---

[28] *R. v. Stinchcombe* 1991 CarswellAlta 559, 1991 CarswellAlta 192, [1991] 3 S.C.R. 326, 68 C.C.C. (3d) 1, [1991] S.C.J. No. 83 (S.C.C.). See also the cases cited in notes 60 and 61, *infra*, and accompanying text.

[29] Rare recognition of the need to apply the national standards was the basis of the decision in *R. v. Oler*, 2014 ABPC 130, 2014 CarswellAlta 1042, [2014] A.J. No. 669 (Alta. Prov. Ct.). It dealt with the disclosure and admissibility of maintenance and other records concerning the Intoxilyzer 5000C, in relation to charges of impaired driving and "over 80" (ss 253(1)(a) and 253(1)(b) of the *Criminal Code*, *supra* note 17).

[30] *The Constitution Act*, 1982, Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

automobiles in compliance with their many standards and laws. The more complex the technology, and the more our lives are dependent upon it, the more complex and voluminous must be the size and complexity of the legal infrastructure of laws, appliers, and enforcers needed to regulate its use. Society must pay that price, otherwise using that technology will cause a lot of damage, and often danger.

"Records management law" will have to be a major area of the practice of law because of: (1) the heavy dependence of laws and human activities upon electronic records; (2) records are the most frequently used kind of evidence in litigation and other legal proceedings; and (3) the complete dependence of electronic records upon the complex technology that is ERMS technology. The problems created by the inadequate legal infrastructure applicable to that technology can be solved by the innovations developed in this article. Further, the "due diligence" required of the records management lawyer will greatly facilitate their efficacy.

## V. GUIDELINES FOR ELECTRONIC DISCOVERY PROCEEDINGS

Such guidelines must emphasize the great differences between: (1) the laws and practices based upon an electronic record stored in an electronic storage device as part of an ERMS; and (2) those based upon a pre-electronic paper record in a file drawer. References to the electronic records provisions of a local Evidence Act should include an explanation of the "system integrity concept," as defined in international or authoritative local standards such as Canada's National Standards of Canada for electronic records management.[31] They provide a definition based upon authoritatively established ERMS procedures, the application of which ensures the use of reliable records as evidence.

In Canada, the predominant text controlling electronic discovery proceedings is the first of the four *Sedona Canada* texts,[32] Sedona Canada

---

[31] The third *Sedona Canada* text, *The Sedona Canada Commentary on Practical Approaches for Cost Containment*, *infra* note 32, refers (at p 26) to the national standard *72.34*, as one in a list of documents, "providing best practices and advice." For experts in ERMS technology it is a "command document" and not merely a "helpmate of good advice." The national standards state what records management policies "shall" include, not what they "could" include. Far better to impose the objective, authoritative standards of the records management profession, instead of the subjective, unauthoritative "reasonable and advisory" choices of the legal profession. And under the heading "A Records Management Policy could also include" (p 14) are suggestions without reference to authoritative standards, as to what should be in such a "records management policy." "Could" is not an appropriate word for such "policy" statements, unless the optional nature of such suggestions is authoritatively explained.

[32] The four *Sedona Canada* texts concerning electronic discovery are:

(1) *The Sedona Canada Principles—Addressing Electronic Discovery* (January 2008), online: The Sedona Conference, <http://www.thesedonaconference.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

Principles-Addressing Electronic Discovery, (hereinafter *Sedona Canada*). In the province of Ontario, its application is mandatory.[33] In Canada's other jurisdictions it is the leading authoritative guideline.[34] It lacks an adequate

---

LexUM (at the University of Montreal), online: < http://www.lexum.umontreal.ca/e-discovery > .And see also Ken Chasse, "Electronic Discovery—*Sedona Canada* is Inadequate on Records Management—Here's *Sedona Canada* in Amended Form" (2011) 9 Canadian Journal of Law and Technology 135.

(2) 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 > ;

(3) The Sedona Canada Commentary on Practical Approaches for Cost Containment (April 2011), online: < https://thesedonaconference.org/publication/sedona-canada-commentary-practical-approaches-cost-containment-public-comment-version > ;

(4) *The Sedona Canada Principles—Addressing Electronic Document Production* (February 2007), available from the Working Group 7 site of the *Sedona Conference* website; online: < http://www.theSedonaConference.org > . Also helpful are *The Sedona Principles Addressing Electronic Document Production*, Second Edition (June 2007) applicable in the U.S., also available from the Sedona Conference website, online: < http://www.thesedonaconference.org/dltForm?did = TSC_PRINCP_2nd_ed_607.pdf > . What is stated herein is equally applicable to this U.S. text, the two being very similar.
And the *Cooperation Guidance for Litigators & In-House Counsel* (7 June 2011), Sedona Conference (webinar), online: < https://thesedonaconference.org/conference/2011/cooperation-guidance-litigators-house-counsel > . "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. The Sedona Conference website states: "the Sedona Conference will publish a new commentary on June 8 [2014]." 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, 25 May 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/ > .

[33] *Rules of Civil Procedure*, Rule 29.1.03(4): "In preparing the discovery plan, the parties shall consult and have regard to the document titled 'the Sedona Canada Principles Addressing Electronic Discovery' developed by and available from The Sedona Conference. O. Reg. 438/08, s.25." (Operative from 1 January 2010).

[34] Recent examples as to how the *Sedona Canada Principles* text is relied upon are: *Ottawa (City) v. Cole & Associates Architects Inc.*, 2012 ONSC 3360, 2012 CarswellOnt 7204, [2012] O.J. No. 2607 (Ont. Master) at para 21; *Corbett v. Corbett*, 2011 ONSC 7161, 2011 CarswellOnt 14487, [2011] O.J. No. 5415 (Ont. S.C.J.); *Warman v. National Post Co.*, 2010 ONSC 3670, 2010 CarswellOnt 5920, [2010] O.J. No. 3455 (Ont. Master), additional reasons 2010 CarswellOnt 11136 (Ont. Master); *Dykeman v. Porohowski*, 2010 BCCA 36, 2010 CarswellBC 136 (B.C. C.A.) at para 41; *Liquor Barn Income Fund v. Mather*, 2011 BCSC 618, 2011 CarswellBC 1139 (B.C. S.C.) at paras 67-78 and 84-87; and *Gardner v. Viridis Energy Inc.*, 2014 BCSC 204, 2014 CarswellBC 320 (B.C. S.C.) at para 15; *Innovative Health Group Inc. v. Calgary Health Region*, 2008 ABCA 219, 2008 CarswellAlta 736, [2008] A.J. No. 615 (Alta. C.A.) at para 26, additional reasons 2008 CarswellAlta 982 (Alta. C.A.), leave to appeal refused 2008 CarswellAlta 1819, 2008 CarswellAlta 1820 (S.C.C.); *Doucet v. Spielo Manufacturing Inc.*, 2007 NBCA 85, 2007 CarswellNB 551, 2007 CarswellNB 552, [2007] N.B.J. No. 510 (N.B. C.A.) at para 11, reasons in full 2008 CarswellNB 712 (N.B. C.A.); *Saint John (City) Employee Pension*

conceptual foundation because it ignores the interdependent relationships contained within the "triangle of interdependent concepts," which constitute the conceptual foundation for the use of electronic records as evidence. It does not deal with: (1) the "system integrity concept" of the admissibility of the electronic records provisions of the Evidence Acts;[35] (2) the "prime directive," because it doesn't refer to the national standards; or (3) the necessary limitation that must be imposed upon the "proportionality principle" not to allow the costs of curing bad records management to justify a claim of "disproportionality" in answer to demands for further disclosure of records. Otherwise, it provides no protection against the list of records management and software defects set out in sections I and II above.

Because of the dependence of an electronic record upon its ERMS, the rule of admissibility in the Evidence Acts, based upon the phrase "the integrity of the electronic records system," requires proof of the state of records management of the ERMS in which the records in question are stored.[36] Because that "system

---

*Plan v. Ferguson*, 2009 CarswellNB 128, [2009] N.B.J. No. 92 (N.B. Q.B.) at paras 15-16; *Vector Transportation Services Inc. v. Traffic Tech Inc.*, 2008 CarswellOnt 1432, [2008] O.J. No. 1020 (Ont. S.C.J.) at paras 19-25, additional reasons 2008 CarswellOnt 2540 (Ont. S.C.J.); *Commonwealth Marketing Group Ltd. v. Manitoba (Securities Commission)*, 2008 MBQB 319, 2008 CarswellMan 602, [2008] M.J. No. 430 (Man. Q.B.) at para 7, affirmed 2009 CarswellMan 94 (Man. C.A.); *Borst v. Horizon Financial Group Inc.*, 2009 CarswellOnt 5984, [2009] O.J. No. 4115 (Ont. Master) at para 3, R. Brott; *Andersen v. St. Jude Medical Inc.*, 2008 CarswellOnt 6654, [2008] O.J. No. 430 (Ont. Master) at paras 27 and 28, C.U.C. MacLeod.

[35] Examples of such electronic records provisions are: ss 31.1-31.8 of the *CEA*; s 34.1 of the Ontario *Evidence Act*; ss 41.1-41.8 of the Alberta *Evidence Act*; ss 23A-23G of Nova Scotia *Evidence Act*; ss 54-59 of the Saskatchewan *Evidence Act*; and the Yukon *Electronic Evidence Act*. Only these three of Canada's 14 jurisdictions do not have electronic records provisions: British Columbia; Newfoundland and Labrador; and the Northwest Territories.

[36] Judicial recognition that such "records management system" proof is required occurred as early as *R. v. McMullen*, 1979 CarswellOnt 1494, 25 O.R. (2d) 301, 47 C.C.C. (2d) 499 (Ont. C.A.) at p. 309 [O.R.], p. 506 [C.C.C.], whereat Morden J.A., delivering the judgment of the Court, stated: "the nature and quality of the evidence put before the Court has to reflect the facts of the complete record keeping process—in the case of computer records, the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation [authorities then cited, omitted]." However, this "*McMullen* standard" of enlightenment no longer prevails, nor in the case law that cited *McMullen*. However, *McMullen* can be used to refute arguments that the business record provisions (*e.g.*, s 30 of the *Canada Evidence Act* (*CEA*), s 35 of the (Ontario) *Evidence Act*, and s 42 of the B.C. *Evidence Act*, cannot be used to decide issues concerning electronic records, because they were created before the present ERMS technology existed. *McMullen* is a banking records case, but s 29 *CEA*, a banking records provision, was also enacted before the presently used ERMS technology existed, *i.e.*, the difference between: (1) records that are merely electronic impressions upon electronic storage devices, which in turn are merely one part of complex ERMSs of infinite variety and degrees of world-wide electronic connectivity and vulnerability; and (2) pieces of paper sitting in file drawers. The former is completely dependent upon its records system

integrity concept" is not dealt with, that dependence is also not adequately dealt with. Therefore, there is no adequate recognition that the use of electronic records for any "legal" purpose should make relevant issues as to the state of records management. Such issues were not relevant to the use of pre-electronic paper records. Good electronic records management is not just a "helpmate" to adequate discovery and admissibility proceedings, it should be a condition-precedent to the success of those proceedings. *Sedona Canada* is based upon the former, but the latter is required by the nature of electronic records and their ERMS technology and its consequences for the law.

Because the *Sedona Canada* text contains no recognition of the serious defects frequently found in ERMSs, it shows no understanding of the need for an assessment of the quality of records management when determining the adequacy of the use of electronic records in discovery and admissibility of evidence proceedings. Without such assessment, one cannot say which demands are "disproportionate" in regard to that system (*Sedona Canada* Principle 2), and which records are "reasonably accessible" (Principle 5). 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. It shows no awareness that 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.[37]

If an ERMS has such defects, it is not possible to comply with a disclosure request as simple as "produce all records on subject X" with complete certainty as to the accuracy, comprehensiveness, and knowledge of the time, cost, and disruption to be incurred by answering such a 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 guidelines such as *Sedona Canada*. One has to know one's ERMS well, and have it operating well, to know what is disproportionate. Such defects will not be known if system documentation showing the state of an ERMS is not kept or demanded by an opponent. An ERMS should be regularly "internally audited," and periodically independently "externally audited," *inter alia*, for compliance with national or international standards.[38]

---

for everything, but the latter is not affected by its records system in any way—not its existence, accessibility, or the integrity of its data.

[37] The *Sedona Canada Principles* text (*supra* note 32) does contain a short section under the heading, "Reasonable Records Management Policies" (Comment 11.e, p. 38), but it is limited to the faulty destruction and disappearance of records.

[38] This process provides a thorough system analysis and comprehensive certification of compliance with the two National Standards of Canada, *supra* note 7 and accompanying text. Such "certification of compliance" work has been done by experts in records management for many years, but a quicker and less expensive procedure is needed in order to use electronic records as evidence; see below.

There is also an "auditing consequence" for defective records systems. If an accountant in testing the "internal controls" of a records system finds that they are not reliable,[39] an 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. That would provide significant support for 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" has a strong similarity to auditing standards.

An ERMS having the above defects cannot comply with the "prime directive" of Canada's national standards for electronic records management: "An organization shall always be prepared to produce its records as evidence."[40] 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 for any legal proceedings. Therefore, 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 of relevant records to opposing counsel.[41] Therefore clients, before they are parties, need to have their ERMSs ready for discovery demands for proof of compliance with the "prime directive" of the national standards. *Sedona Canada* does not deal with these essential links.

An independent expert certification of "national standards compliance," or a sworn statement to the same effect by a chief records officer, subject to examination, could eliminate such issues. Therefore, *Sedona Canada* should be amended to make records management that is compliant with the national standards mandatory. See section VIII below for the legal infrastructure needed to create a simple procedure for proving such compliance at discovery and at trial.

---

[39] For the "directives and procedures of finance and accounting," see this website of the University of Florida: < http://www.fa.ufl.edu/directives-and-procedures/ > .

[40] *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, para 4.1.2 at p 21, *supra* note 7 and accompanying text.

[41] There are more than 250 specific compliance requirements and tests that records management project teams can apply to determine the level of compliance of an ERMS with the national standards, *supra* note 7. The resulting report indicates the level of compliance found by each test, along with recommendations, and an assessment as to "legal compliance" with legislated records and records management requirements. Such is one of the types of work justifying "records management law" as an area of specialization. It also requires ERMS experts to work closely in conjunction with records management lawyers to maintain clients' continuous compliance with "the prime directive" of the national standards, *i.e.*, "preventive law" and not only "remedial law" services.

Because of its serious defects arising from its inadequate reference to and discussion of ERMS technology, *Sedona Canada* makes bad records management a good litigation strategy, and good records management a bad litigation strategy—particularly so because the "proportionality" Principle 2 of *Sedona Canada*, disproportionate to the worth and importance of what is in dispute, ignores the fact that the "disproportionate" time and cost difficulties claimed to be imposed by an opponent's demands for further production of records are in fact due to the claimant's own bad records management. Therefore the *Sedona Canada* text provides inadequate rules of procedure for electronic discovery proceedings, and their impact upon admissibility of evidence proceedings. Nonetheless, the case law entrenches it in support of legal procedures that create an unacceptably high probability of the use of inadequate records, their production, and their admissibility, and therefore of inadequate "justice."[42]

The above serious defects contained in the *Sedona Canada Principles* will be perpetuated by the second edition, a draft of which is available for comment.[43] In response to my article "The Sedona Canada Principles are Very Inadequate on Records Management and for Electronic Discovery,"[44] I received this comment:[45]

> We have noted your comments that the Principles are "very inadequate" on Records Management and for Electronic Discovery. However, the Principles are not intended to place significant focus on records management (RM) or the importance or desirability of appropriate RM practices so as to be properly prepared for litigation, or on issues related to the integrity of information systems under Evidence Acts, or on the substantive law related to the admissibility of electronic records into evidence. Those issues are all important, but are largely outside the scope of the Principles. The Principles are instead focused on the discovery process in whatever circumstances litigants find themselves in. The Principles take ESI as the parties find it when

---

[42] Therefore representatives of the *Sedona Canada* drafting committee are members of the committee updating the national standards (*supra* note 7). Next, the records provisions of the Evidence Acts should be revised to complete the "triangle of interdependent concepts," and the "triangle of interdependent proceedings," (see the text accompanying notes 25 to 29, *supra*), which are necessary to create a law and practice whose adequacy is explicitly based upon ERMS technology, in place of the present law and practice that ignores it (see the case law in notes 21 and 33, *supra*).

[43] A draft 2nd edition of Sedona Canada has been issued—the "February 2015 Public Comment Version," online: Sedona Conference < https://thesedonaconference.org/publication/The%2520Sedona%2520Canada%2520Principles > .

[44] Online: SSRN < http://papers.ssrn.com/sol3/papers.cfm?abstract_id = 2530515 > . This article is an updated and revised version of my article: "Electronic Discovery—-*Sedona Canada* is Inadequate on Records Management—Here's *Sedona Canada* in Amended Form" (2011) 9 Canadian Journal of Law Technology 135.

[45] From members of The Sedona Conference, Working Group 7 (Sedona Canada) Steering Committee, received by email message on 19 December 2014.

> litigation arises, not as how it could be were parties to pay more appropriate attention to the importance of proper RM and information governance in the first place. The forthcoming new edition of the Principles will make that clear.

This comment ignores the requirement in the electronic records provisions of the Evidence Acts that admissibility of electronic records requires proof of the "integrity of the electronic records system in which the records are recorded or stored." To serve its purpose of reducing the time and cost of trials, discovery should require disclosure of information as to whether such requirement can be proved, that is, information as the state of records management. Proof of such "integrity" requires proof of the state of compliance of the record system with an authoritative standard of records management. The most authoritative of such standards are those that the Standards Council of Canada has proclaimed to be National Standards of Canada.

In footnote 243 of the draft second edition of the *Sedona Canada Principles*, a number of standards for electronic records management are listed, including Canada's National Standards, which should be the only standards referred to; other standards are not of equal authority. Showing compliance with them may assist in achieving admissibility, whereas compliance with the national standards should definitely satisfy the "proof of records system integrity" requirement of the admissibility rule in section 31.2(1)(a) of the *Canada Evidence Act*.[46] The electronic records provisions should be amended to make that clear.[47] The Appendix below provides suggested amendments for section 30 and the electronic records provisions of the *Canada Evidence Act*.[48]

The National Standards are *Electronic Records as Documentary Evidence* CAN/CGSB 72.34-2005 and *Micrographics and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93 (as amended to 2000). Footnote 243 shows a lack of understanding of Canada's national standards system, in particular the disciplining of the procedure used to obtain a proclamation by the Standards Council of Canada of draft standards to be National Standards of Canada. Footnote 243 also compounds this error by stating: "These standards are not mandatory." In fact, it is not possible to prove the "integrity" of an ERMS without applying such standards. To use the expert witness analogy set out above, footnote 243 amounts to saying that in presenting expert opinion evidence, it is not mandatory that the expert have adequate qualifications because such qualifications are not mandatory. Such review of the state of compliance of ERMSs with the national standards is necessary and should not be left to the trial. Such determination by way of an "admissibility of evidence

---

[46] *CEA*, *supra* note 2.

[47] See the Appendix, below, as to how I would amend the electronic records provisions of the *Canada Evidence Act*, and as well render s 30 compatible with those amendments. The Evidence Acts of the provinces and territories should similarly be amended. The relevant provisions of Book 7 of the *Civil Code* of Quebec would not need to be amended.

[48] *CEA*, *supra* note 2.

procedure" is much more time consuming than would be a mandatory requirement to produce such information at discovery.

Given the lack of knowledge of ERMS technology by lawyers, the quoted comment and footnote show that the drafters have not adequately accommodated the great difference between electronic records technology and pre-electronic paper records technology; the difference between an electronic record being like a drop of water completely dependent for its existence, accessibility, and integrity upon the pool of water that is its ERMS, and a pre-electronic piece of paper in a file drawer. ERMS technology is very different and much more complex than pre-electronic paper records technology. Its improper use is very likely to produce inadequate evidence. The state of use of pre-electronic paper records system technology cannot affect the existence, accessibility, and integrity of a paper record—paper records are not affected by the state of their file drawers nor by the state and use of all the file drawers in a paper records system, which is the reason why records system issues are absent from the pre-ERMS case law. They definitely should not be absent, as they are, from the ERMS case law concerning discovery and admissibility of electronic records. Therefore there is very likely to be an unacceptably high probability of judgments being based upon inadequate and faulty evidence if the use of ERMS technology to produce records as evidence is not adequately reviewed.

The means of detecting judgements that are unjust because of the inadequacies of the evidence upon which they are based are very poor, and therefore instances wherein they are detected are very infrequent and unusual.[49] Therefore, it is only adequate rules of prevention, applicable to discovery and admissibility proceedings, that can provide a sufficient opportunity to apply safeguards against inadequate records being used as evidence. Unfortunately, the second edition will not correct this serious inadequacy of the first edition.

Also, the second edition will not direct sufficient attention to: (1) the serious, common defects of records management and software listed in the first two sections of this article, and their considerable impact upon the difficultly of determining the adequacy of disclosure made in discovery proceedings; or (2) the fact that the admissibility of records is dependent upon proof of the "integrity" of the records systems in which they are stored, which requires proof of the compliance of such records systems with the National Standards of Canada for electronic records management. Information in relation to such issues should be required in discovery proceedings so as to reduce the time taken by them at trial. If they were a required part of discovery proceedings,[50] they could often make summary judgment procedures available.[51]

---

[49] As an example of the unusual circumstances required to detect faulty evidence producing the conviction of an innocent man, see, *R. v. Hanemaayer*, 2008 ONCA 580, 2008 CarswellOnt 4698, 234 C.C.C. (3d) 3 (Ont. C.A.), and the review of the faulty evidence and its detection long after the sentence had been served, beginning at page 62 of the article by Ken Chasse, "Plea Bargaining is Sentencing" (2009) 14 Canadian Criminal Law Review 55.

## VI. THE DIVISIONS OF WORK WITHIN THE NEW FIELD OF "RECORDS MANAGEMENT LAW" FOR THE "RECORDS MANAGEMENT LAWYER"

Because of the great dependence of laws and almost everything that we do upon electronic records, "records management law" will become a major field of the practice of law. The efficacy of that heavy dependence should not be as seriously weakened as it is by the defects set out above in the first two sections. Therefore the "records management lawyer" will have to become an established specialist. Lawyers and experts in ERMS technology should be working closely together: (1) to compensate for the present inadequacies of the law and practice concerning records; (2) to cope with legal proceedings, and avoiding them; (3) to compensate for the general lack of knowledge of ERMS technology by the legal profession, particularly so by in-house counsel; and (4) to provide good records management in both its records management and legal components. The following subsections will discuss the resulting divisions of work of the "records management lawyer".

### (a) Legal Opinions

Legal options as to the ability of electronic records management systems (ERMSs) to satisfy the electronic records demands as to:

(a) electronic discovery;
(b) admissibility of electronic records as evidence;
(c) electronic commerce laws;
(d) privacy and access to information laws;
(e) records requirements of the major tax laws; and
(f) compliance with the national standards of Canada for electronic records management; (referred to as *72.34* and *72.11)*.[52]

Because ERMSs are catch-all reservoirs of electronic records, they reflect all significant changes within the organizations that use them. Such legal opinions would therefore be routinely provided at least once annually, and also in relation

---

[50] Making the production of such information as to the state of compliance with the national standards mandatory at discovery proceedings would be greatly facilitated if the electronic records provisions of the Evidence Acts expressly stated that the admissibility of records could be obtained by proving such compliance of the ERMS in which the records are stored.

[51] As to when summary judgment is appropriate, see: *Hryniak v. Mauldin*, 2014 SCC 7, 2014 CarswellOnt 640, 2014 CarswellOnt 641 (S.C.C.); and *MacDonald v. Chicago Title Insurance Co. of Canada*, 2014 ONSC 7457, 2014 CarswellOnt 18249 (Ont. S.C.J.), additional reasons 2015 CarswellOnt 2324 (Ont. S.C.J.), which deal with Rule 20 of the Ontario Rules of Civil Procedure.

[52] *Supra* note 7. Such opinions would assure compliance with "the prime directive" of the national standards: "an organization shall always be prepared to produce its records as evidence." (See text accompanying note 24, *supra*).

to every significant change to an ERMS. They would also accompany reports of experts in ERMS technology. Part of such reports would deal with compliance with standards such as the National Standards of Canada for electronic records management. Such legal opinions would also deal with special records requirements imposed by regulatory agencies or specialized legislation applicable to particular industries or professions.[53]

### (b) Aiding Clients to Develop Indexing Systems for all of their Records

This is the solution to the high cost of the "review" stage of electronic discovery.[54] Database discipline and indexing should be applied to *all* significant records within a client's ERMS, and not just to the information recorded in its financial records. If fully used, a well-indexed ERMS can provide as much useful information for an organization as its financial records do. The "records management law" specialist teaches clients indexing and the database discipline that it makes possible. Then, the accessing and "reviewing" of clients' records for relevance and privilege could be done together as one operation by the litigation or records management lawyer, using the speed of electronic searching applied to the client's indexing system. Clients would not need to be involved. The reading of records for relevance and privilege would be greatly reduced. Similarly, when legal research is done by lawyers (or, more often, by their students), the accessing and reviewing of relevant materials is much reduced in time and cost because: (1) of the highly indexed, headnoted, abstracted, and summarized nature of legal materials; (2) the searching is done by experts in legal research—lawyers and their students; and (3) the searching is done with the speed provided by electronic searching. Thus the "high cost of the review stage problem" would disappear if such benefits were brought to clients' ERMSs. Such would be part of the "due diligence" work done by a lawyer specialized in records management law, or ensure that it was done, and to instruct the client as to the needed database preparation. Clients will do it if shown that it will help fulfill their goals.

The National Standard of Canada, *Electronic Records as Documentary Evidence* imposes the following indexing requirements, which would be part of

---

[53] Working with experts in electronic records management, I have written such opinions. They are part of the reports provided to institutional clients that have large ERMSs. All such reports should provide a certification of an ERMS as being in compliance with the national standards, *supra* note 7. Experts in records management have done such work for many years. One series of such reports that I worked on was the result of a provincial government's requests that some of the province's universities have their ERMSs so certified.

[54] See Ken Chasse, "Solving the High Cost of the 'Review' Stage of Electronic Discovery," and other relevant articles listed on my SSRN author's page, online: < http://ssrn.com/author = 1398484 > . This article can also be accessed from the *Slaw* blog as "Solving the High Cost of the 'Review' Stage of Electronic Discovery" (17 April 2014) SLAW (blog), online: < http://www.slaw.ca/2014/04/17/solving-the-high-cost-of-the-review-stage-of-electronic-discovery/ > .

the "quality control" and "due diligence" functions of the records management lawyer:[55]

> **6.5.1 General**
> Indexing is a vital part of storing and retrieving information on an RMS [records management system] program. Indexing, which can be automated or manual, shall include the following functional requirements:
>
> a) the specification of the indexing methodology and scheme used;
> b) type and structure of indexing used, including the primary index element as well as all additional levels of indexing;
> c) methods for performing quality control of indexing;
> d) procedures in place to amend inaccurate index data;
> e) where an index entry references deleted or expunged information, the index shall reflect the deleted or expunged status; and
> f) procedures for performing quality assurance of the indexing.
>
> **6.5.2 Index retention, rebuilding and recovery**
> Index data shall be kept for the retention period of the SRI [set of recorded information] to which it relates. The procedures for rebuilding an index, changing an index structure, and recovering a damaged or faulty index shall be authorized and documented, as well as all results of such events.

Thus, the same three features that facilitate legal research can be brought to clients' records management, their doing business, preparation for litigation, and eliminating the high cost of the "review stage" of electronic discovery. Therefore, a "proportionality" concept is not needed to limit the amount of legal research that one party inflicts upon an opposing party by way of raising many issues and bringing many applications before and during trial. Similarly, a client doesn't give its accountant thousands of records containing financial information and say, "here, you make up the necessary financial records, and then do the audit." Instead, the client does the sorting of financial information into its financial records on a continuous, daily basis. Accessing, sorting, and reviewing records is far more cost-efficiently done by way of a "front end" indexing of records than by a "back end" reading of records.

Also, indexing is well justified because searching a database of texts (instead of its index, if there is one) is very inaccurate. Quoting from a recent article:[56]

> Indeed, we know that current e-discovery search methods are not sufficient to overcome the digital tsunami: the most common methods

---

[55] *72.34*, *supra* note 7, contains these indexing requirements in section "6.5 Indexing," at page 23. I expect the next edition of this standard, currently being drafted, will more explicitly state that all records within a records system should be indexed.

[56] Victoria L Lemieux & Jason R Baron, "Overcoming the Digital Tsunami in e-Discovery: is Visual Analysis the Answer?" (2012) 9 Canadian Journal of Law and Technology 33 at 35.

> currently used in e-discovery—keyword searching and linear review—are increasingly ineffective for the massive volumes of data that must be sifted through for each case. There have been a number of studies highlighting the limitations of existing search and retrieval techniques. In one study lawyers overestimated the effectiveness of their keyword-based search strategies by as much as 55%. Dabney (1986), Bing (1987) and Schweighofer (1999) all provide in-depth reviews of the limitations of full text searching for legal documentation. More recently, a multi-year study evaluating the efficacy of various search methods known as the "TREC Legal Track" demonstrated that traditional Boolean search methods failed to find up to 78% of relevant documents that other automated search methods accounted for (Tomlinson et al, 2008). . . . .
>
> All of these prior reports and studies are in line with results of an online survey of legal and technical professionals in the UK and two roundtable discussions on e-discovery conducted by PwC [PricewaterhouseCoopers] indicating that keyword searching is increasingly untenable. Panelists noted the difficulties of choosing key words, reporting that "[e]ven if you have a brilliant, absolutely focussed search, you are still going to end up with too many documents to review and within those there will still be a very large proportion of irrelevant material." Data volumes are quickly becoming such that even with the best keyword search terms and an army of reviewers, it could still take months or years to sift through all the data and there would still be no guarantee of satisfactory results. New approaches are therefore very much needed. [footnotes omitted]

Is the efficacy of "predictive coding" and other "technology assisted review" devices, used to reduce the cost of the "review" stage of electronic discovery, undermined by their reliance on keyword searching strategies?[57]

### (c) Provide the "Due Diligence" to Maximize the Efficacy of Electronic Discovery and Admissibility Proceedings

Currently, these proceedings do not provide any incentive for records management that is compliant with the national standards. The "proportionality" principle 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 ERMSs. The parties have control of the records systems from which the records "discovered" come, including the probability of serious defects in those systems. Potentially, they have more control over the adequacy and fairness of electronic discovery than do their lawyers.

It follows that there should be a "duty of due diligence" that the lawyers for the parties perform so as to provide a legally recognized power of assurance that the records systems are capable of providing adequate and fair discovery. Such is analogous to similar "due diligence" requirements of lawyers in other fields of

---

[57] *Infra* note 67 and accompanying text.

law and practice.[58] The records management law specialist could provide that necessary "due diligence." That could forestall an order for the examination of a party's ERMS by a third party expert, when such becomes the practice of the courts. Such examination would determine the state of compliance of that ERMS with authoritative standards of electronic records management. Either by way of effective due diligence or such court orders, such compliance must be made part of the laws of evidence, electronic discovery, admissibility, the proportionality principle, and of the *Sedona Canada* texts. Non-compliance should give rise to a rebuttable presumption of a lack of "system integrity," and therefore of inadmissibility and inadequate discovery. That is the solution to the present problems of electronic discovery proceedings.

### (d) Knowledge of Case Law so as to Eliminate the Time-Consuming and Therefore Expensive Challenges (Squabbles) and Court Applications Concerning the Adequacy of "Production" During Discovery Proceedings

If there were no "confidentiality and privileged information" issues, opposing counsel could be allowed to search the opposing party's records system's indexed database.[59] That would confirm that adequate searching and production had been made by an opposing party, and that that party's records system was in compliance with the National Standards of Canada for electronic records management, or otherwise capable of providing adequate access to all relevant records. Such preparation for and monitoring of searches by opposing counsel would be part of the work of the records management lawyer. Criminal procedure would have to have a counterpart with which to cope with its version

---

[58] For example: (1) the required due diligence in regard to the disclosure of financial assets for the making of family law separation agreements. It has been held by the Supreme Court of Canada that a lawyer's due diligence is needed because, "Non-disclosure of assets is the cancer of matrimonial property litigation": *Leskun v. Leskun*, 2006 SCC 25, 2006 CarswellBC 1492, 2006 CarswellBC 1493, [2006] S.C.J. No. 25 (S.C.C.), Binnie J. for the Court, at para 34. And, (2) due diligence required for the use of cloud computing (a type of third party service provider for electronic data storage and processing); see Law Society of British Columbia, *Report of the Cloud Computing Working Group*, Appendix 1 "Due Diligence Guidelines" (27 January 2012) at p 29.

[59] Would such be comparable to "rummaging through an opponent's filing cabinet"? See *Borst v. Horizon Financial Group Inc.*, 2009 CarswellOnt 5984 (Ont. Master) at para 5: "In the ordinary discovery process, it is the responsibility of each party to review all of its documents and to deliver copies of all Schedule 'A' documents to the other parties. I agree with the Court of Appeal of Alberta in *Innovative Health Group Inc. v. Calgary Health Region*, 2008 ABCA 219, 2008 CarswellAlta 736 (Alta. C.A.) at para 58, additional reasons 2008 CarswellAlta 982 (Alta. C.A.), leave to appeal refused 2008 CarswellAlta 1819, 2008 CarswellAlta 1820 (S.C.C.): 'A litigant does not have the right to rummage through an opponent's filing cabinets to see if it can find something interesting. . . .' The Court of Appeal analogized the request for the electronic data to a request to inspect the filing cabinet and the court deemed the request to be a fishing expedition and denied the request." And therefore, at para 62 holding that: "the case management judge's decision to allow production and copying of the imaged hard drives is overturned."

of the same problem.[60] Knowledge of all case law, including that concerning search and seizure, will be required.[61]

Such "searching by opposing counsel" would be comparable to providing an adequate opportunity to cross-examine opposing witnesses. Electronic records and their records systems have to be challenged as to their "integrity" and adequacy just as much as do witnesses.[62] Because the "system integrity concept" is always operative in any legal proceedings concerning electronic records as evidence, such provisions should be added to the Evidence Acts of British Columbia, the Northwest Territories, and that of Newfoundland and Labrador.

Due to the frequency of issues concerning the protection of confidential information and privileged records, searching an opposing party's records system

---

[60] In its decision on disclosure and discovery in criminal proceedings, *R. v. McNeil*, 2009 SCC 3, 2009 CarswellOnt 116, 2009 CarswellOnt 117, [2009] 1 S.C.R. 66, 238 C.C.C. (3d) 353, [2009] S.C.J. No. 3 (S.C.C.), the Supreme Court of Canada cites (at paras 29 and 44) the importance of "preventing unnecessary applications for production", "conserving scarce judicial resources", and "the court must play a meaningful role in screening applications 'to prevent the defence from engaging in speculative, fanciful, disruptive, unmeritorious, obstructive and time-consuming' requests for production," (*O'Connor*, at para 24, quoting from *R. v. Chaplin* (1994), 1994 CarswellAlta 1069, 1994 CarswellAlta 1070, [1995] 1 S.C.R. 727 (S.C.C.) at para 32). However, the Supreme Court's decisions emphasize as well the need to facilitate "full answer and defence"; see: *R. v. Quesnelle*, 2014 SCC 46, 2014 CarswellOnt 9195, 2014 CarswellOnt 9196, [2014] S.C.J. No. 46 (S.C.C.); *R. v. Bjelland*, 2009 SCC 38, 2009 CarswellAlta 1110, 2009 CarswellAlta 1111, [2009] S.C.J. No. 38 (S.C.C.); *R. c. Taillefer*, 2003 SCC 70, 2003 CarswellQue 2765, 2003 CarswellQue 2766, [2003] 3 S.C.R. 307 (S.C.C.); *R. v. Shearing*, 2002 CarswellBC 1661, 2002 CarswellBC 1662, [2002] 3 S.C.R. 33, 165 C.C.C. (3d) 225, 2 C.R. (6th) 213 (S.C.C.); *R. v. Mills*, 1999 CarswellAlta 1055, 1999 CarswellAlta 1056, [1999] 3 S.C.R. 668, 139 C.C.C. (3d) 321, 28 C.R. (5th) 207, 180 D.L.R. (4th) 1 (S.C.C.); *R. v. O'Connor*, 1995 CarswellBC 1098, 1995 CarswellBC 1151, [1995] 4 S.C.R. 411, 103 C.C.C. (3d) 1, [1995] S.C.J. No. 98 (S.C.C.); *R. v. Chaplin* (1994), 1994 CarswellAlta 1069, 1994 CarswellAlta 1070, [1995] 1 S.C.R. 727, 96 C.C.C. (3d) 225 (S.C.C.); *R. v. Stinchcombe*, 1991 CarswellAlta 559, 1991 CarswellAlta 192, [1991] 3 S.C.R. 326, 68 C.C.C. (3d) 1, [1991] S.C.J. No. 83 (S.C.C.). See also note 28, *supra,* and accompanying text.

[61] For example, in *R. v. Vu*, 2013 SCC 60, 2013 CarswellBC 3342, 2013 CarswellBC 3343, [2013] 3 S.C.R. 657 (S.C.C.), the Court held that the traditional search warrant did not give authority to search a computer as though it were just another container or receptacle found on the premises. And in *R. v. Fearon*, 2014 SCC 77, 2014 CarswellOnt 17202, 2014 CarswellOnt 17203 (S.C.C.), the Court held that a cellphone (mobile) could be searched on arrest without a warrant, with the result that text messages and photos found in the cellphone could be used as evidence.

[62] In s 31.2(1)(a) of the *Canada Evidence Act*, the "system integrity concept" is set out in these words: "the best evidence rule in respect of an electronic document is satisfied (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored." And in s 34.1(5),(5.1) of the Ontario *Evidence Act*, in these words: "(5) 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 an 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."

will seldom be possible. Therefore, examination-on-discovery of opposing parties, including their affidavits, is the necessary substitute. Now, issues as to the state of ERMS management are ignored by lawyers, barred by judges, and therefore, with but very rare exception, absent from Canada's case law on electronic discovery.[63]

### (e) Working with Experts in ERMSs

The "records management lawyer" will be required to perform contracts for the repair, alteration, and creation of ERMSs, and the providing of legal opinions as to client organizations' ability to comply with the records requirements of the six areas listed above on page 81. Now, such contracts are obtained by competitive bidding by independent groups of records management experts.[64] Therefore, they are providing "legal information" where lawyers should be providing legal advice.

Instead, that "bidding for contracts system" should be displaced by making such work part of law firms' continuing legal services to clients, *i.e.*, a "preventive law" service, instead of only "remedial law" services concerning litigation and disputes. ERMS experts and records management lawyers should be working closely together.[65] Those organizations using the services of a records

---

[63] Examples of such "rare exception" case law that deals with such ERMS issues are discussed in notes 81 and 82 and accompanying text, *infra*.

[64] Such offered contracts "put out to tender" are listed on websites such as MERX, *About Merx* (website), online: < https:// www.merx.com > . It states: "MERX is the most complete source of Canadian public tenders, Agencies, Crown & Private corporations, U.S. tenders and private-sector construction news available in Canada. MERX has leveled the playing field so that businesses of any size can have easy and affordable access to billions of dollars in contracting opportunities with the Government of Canada (GC), participating provincial and municipal governments, the U.S. Government, state and local governments, and the private sector. MERX presently offers its suppliers four services..." It then describes the services under these four headings: Canadian Public Tenders Service; Agencies, Crown & Private corporations Service; U.S. Tenders Service; and Private Construction Service. Such proffered contracts are generated by commonly used rules of organizations requiring any work or service costing more than $5,000 to be put out "to tender." Therefore, such websites are closely watched by ERMS experts.

[65] For example, the Law Society of Upper Canada's (LSUC's) *Professional Regulation Committee's Report to Convocation on Alternative Business Structures* (27 February 2014) recommends consultation as to allowing law firms to provide non-legal services in conjunction with legal services. See also the LSUC's News Release of February 27th announcing such consultation and requests for feedback, online: LSUC < http:// http:// www.lsuc.on.ca/latestnews.aspx?id = 11610 > . Therefore see also this statement on Alternative Business Structures, (online: < http://www.lsuc.on.ca/ABS/ > ): "the Law Society released Alternative Business Structures and the Legal Profession in Ontario: A Discussion Paper on 24 September 2014, (online: < http://www.lawsocietygazette.ca/ treasurers-blog/abs-creating-dialogue/ > , to seek input from lawyers, paralegals, stakeholders and the public about Alternative Business Structures (ABS)." Comments and requests to attend meetings were to be sent to, < abs.discussion@lsuc.on.ca > by 31 December 2014. See my response, Ken Chasse, "What a Law Society Should Be-A

management lawyer would not need to put such work out for competitive bidding.

### (f) Assisting litigation counsel in dealing with electronic discovery problems, particularly its "review" stage.[66]

The most helpful assistance a "records management lawyer" could provide would be to assist or teach conducting the review stage by use of predictive coding technology.[67] As to the cost, rules of electronic discovery will be enacted with which to punish parties with "sanctions"[68] for not maintaining their electronic records systems in compliance with Canada's National Standards for electronic records management[69]—to sanction when inadequate records management interferes with electronic discovery or otherwise damages parties' interests.[70] Such compliance greatly reduces the cost of, and increases the effectiveness and fairness of, doing anything that can be done with electronic

---

Response to the Law Society of Upper Canada's Alternative Business Structures Discussion Paper of September 24, 2014" (pdf), at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549960>.

66 A beginning of this specialized practice is the appointment of electronic discovery expert lawyers by larger law firms. See for example this announcement on August 6, 2013, by Borden Ladner Gervais LLP, a law firm having more than 750 lawyers across Canada: "BLG hires Canada's leading electronic discovery lawyer," Martin Felsky; online: <http://www.blg.com/en/newsandpublications/news_1439>. Along with the other functions set out in this section, the work of the "electronic discovery lawyer" will become that of the "records management lawyer."

67 "Predictive coding" is a document review technology that allows computers to predict particular document classifications (such as "responsive" or "privileged") based upon coding decisions made by those knowledgeable as to the subject matter. In the context of electronic discovery, this technology can find key documents faster and with fewer human reviewers, thereby saving much time to conduct document review for finding relevant and potentially privileged documents. A detailed description of the use of predictive coding devices is found in *Dynamo Holdings Ltd. Partnership v. Commissioner of Internal Revenue* (September 17, 2014), Doc. 2685-11, 8393-12 (U.S. T.C.), online: <http://goo.gl/NiY7XY> (click "available here" at the bottom of the page). It is also mentioned in, *L'Abbé v. Allen-Vanguard Corp.*, 2011 ONSC 7575, 2011 CarswellOnt 15489, [2011] O.J. No. 5982 (Ont. Master) at para 23: "Various electronic discovery solutions are available including software solutions such as predictive coding and auditing procedures such as sampling." But whether predictive coding can make common sized litigation affordable to a majority of the population is yet to be decided. Given the substantial criticism of keyword searching (*supra* note 56 and accompanying text), is predictive coding's efficacy undermined by relying upon keyword search strategies?

68 See *Sedona Canada* Principle 11 as to the definition and use of "sanctions," in: *Sedona Canada Principles—Addressing Electronic Discovery* at p 36. The four *Sedona Canada* texts concerning electronic discovery are listed in note 32, *supra*.

69 *Supra* note 7 for those national standards.

70 Indications of such lack of compliance are the common serious defects frequently found in ERMSs, listed at the opening of this article.

records.[71] Therefore, by thus incorporating issues as to "the quality of records management" into the law of electronic discovery, discovery is made more effective and is much better equipped to control its costs.[72] Due to the cost of such litigation, the "electronic discovery lawyer" will evolve to become the "records management lawyer," and a support service available to all lawyers, if litigation is not to be restricted to the rich.

### (g) Providing Clients with "Preventative Legal Services"

Providing clients with "preventive legal services" instead of only remedial legal services, *i.e.*, legal services that prepare the client for litigation before it happens, and for examinations of ERMS procedures by government officials and regulatory bodies. Of particular importance, because ERMSs are constantly changing yearly opinions should be provided as to compliance with the national standards for electronic records management, especially "the prime directive"—"an organization shall always be prepared to produce its records as evidence".[73] The "records management lawyer" must make clients sufficiently knowledgeable as to:

(1) the records management and legal requirements of the national standards;
(2) all the laws and regulations that create records requirements, particularly the laws of evidence, electronic discovery, privacy, and access to information, electronic commerce, and taxation;
(3) the legal consequences of electronic records management systems changing as their organizations and operations change; and,
(4) the consequences of more laws based upon technology, and the fact that every electronic communication and service creates a record that is potentially evidence and relevant to some legal service.

### (h) To Make Litigation Available to People of Average Incomes

The "records management lawyer specialist" should be a support service available to all law firms. Now, the cost of the "review" stage of electronic discovery proceedings puts litigation that involves large volumes of records beyond the means of the majority of the population (even if the use of

---

[71] 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 with the National Standards of Canada, *supra* note 7.

[72] The high cost of electronic records discovery greatly aggravates the "unaffordable legal services problem," making litigation and other legal services unaffordable for the majority of Canada's population. For example, view the video of Beverley McLachlin, Chief Justice of Canada, Access to Civil Justice Colloquium (10 February 2011), University of Toronto, Faculty of Law (video), online: < https://hosting2.desire2learncapture.com/MUNK/1.aspx >. See also, my papers on the SSRN (Social Science Research Network) concerning this "access to justice" problem, online: < http://ssrn.com/author = 1398484 >.

[73] *Supra* note 7, and *supra* notes 52 and 53 and accompanying texts.

"technology assisted review" software, such as incorporated within predictive coding devices, becomes routine). It is the best strategy for adequately reducing the cost of electronic discovery in particular, and litigation in general.

Now, instead of the legal profession providing such legal services, the records management profession is providing general legal information, including information on the "legal requirements" of the national standards for electronic records management,[74] and not involving lawyers in their work.[75] Their clients don't realize that they should be using such legal services. Such is also true of their legal departments, as is shown by the absence of ERMS issues in almost all case law and guidelines concerning the use of electronic records as evidence, including the four *Sedona Canada Principles* texts.[76]

One of the reasons why the "prime directive" of the national standards requires records systems to always be ready to provide their records as evidence is that the state of records management when records are created and stored, and continuously thereafter, is always determinative of their continued existence, accessibility, and integrity for electronic discovery proceedings and their ability to be admissible evidence. "Records integrity" is not a requirement for merely a single point in time, but rather a continuous requirement up to the time records are to be used for any legal purpose. Therefore, bringing an ERMS into compliance with the national standards provides no information as to the

---

[74] *Supra* note 7. Because the "legal" requirements of *72.11* are out of date, such "legal advice" by non-lawyers is very likely to be inadequate. However, *72.11* remains the industry standard for imaging (conversion of paper records to digital storage). Because many organizations still have large volumes of pre-electronically created paper records, imaging is a big industry. Therefore, one of the purposes of the electronic records provisions of the Evidence Acts is to give such digitized records the status of "originals" (*e.g.,* s 31.2(1)(a) of the *Canada Evidence Act*, and s 34.1(5),(5.1) of the (Ontario) *Evidence Act*. Both national standards (*72.34* and *72.11*) were drafted with the advice of experts in the law concerning the use of records as evidence. Both standards are now under revision, with completion scheduled for late in 2015. Review and then promulgation by the Standards Council of Canada of the new editions will follow early in 2016.

[75] I am a rare exception. Because institutional records managers who put contracts out to tender are not used to having a legal opinion accompany the work of experts in ERMSs ("because we have had no trouble before"), I include a paper in the bid for the contract that explains why a legal opinion is necessary (published as: "Why a Legal Opinion is Necessary for Electronic Records Management Systems," (2012) 9 Digital Evidence and Electronic Signature Law Review 17 (U.K.; an "open source" journal providing free .pdf downloads), online: < http://journals.sas.ac.uk/deeslr/article/view/1986 > . Note that the writing style and body of the text are intended for readers who are not lawyers. Therefore it is the footnotes that contain all of the authorities and other references that lawyers would be looking for. Although the contracting institution's records manager would be reviewing the submitted bids, I assume that bids would be passed on to the institution's legal department. The legal profession should institute a project that informs such records managers and their legal departments that the "legal information" of experts in records management does not fulfill the need for a legal opinion.

[76] *Supra* note 32, and notes 79-81 and accompanying text, *infra*.

continued existence, accessibility, and integrity of its records before compliance was achieved.

## VII. THE "SYSTEM INTEGRITY CONCEPT"

Nonetheless, lawyers and judges on reading the above paragraphs might answer incredulously, "the high cost of electronic discovery must be reduced; therefore the issues must be limited to the electronic records themselves, and only on significant evidence, to no more of the records system than particular devices that may contain them."

A law based upon a technology, however, cannot ignore the nature, weaknesses, and dangers of that technology and fulfill its purpose. Electronic technology and paper technology are different technologies. The former is not merely a sped-up and more conveniently used version of the latter. Electronic discovery cannot be made as simple and inexpensive as pre-electronic paper discovery because: (1) the integrity of an electronic record is dependent upon the integrity of its ERMS, but the integrity of a pre-electronic paper record is not affected by the state of its records management system; (2) electronic technology has made the making of records much more convenient, less expensive, and time-consuming, and most often automated, therefore ERMSs quickly become voluminous; and, (3) every electronic communication creates a record. The current case law reduces costs by reducing the competence of the discovery proceedings by which records are produced and determined to be admissible or inadmissible.

The "system integrity concept" states that the integrity of an electronic record is dependent upon the integrity of the ERMS in which it is stored—"records integrity" requires proof of records system integrity.[77] Therefore, regardless what the applicable Evidence Act and its case law state or don't state, whenever electronic records are used as evidence, it is an operative fact that an electronic record is dependent upon its ERMS for everything. The requirements of admissibility should make mandatory the producing of such corresponding information during electronic discovery proceedings, *i.e.*, information as to the state of "system integrity" of the ERMS in which the records produced have been "recorded or stored."

A major purpose of electronic discovery proceedings being to "discover" records that might be used as evidence, requests should be allowed to be made of an opposing party for information as to the level of "integrity" and compliance of the ERMS in which the records being produced are recorded or stored with the national standards. That would make issues of records management relevant to electronic discovery. In fact, such issues are strongly avoided by restricting orders for production to specific records and their electronic devices, as

---

[77] See for examples: s 31.2(1)(a) of the *Canada Evidence Act*, s 41.2(1)(a) of the *Alberta Evidence Act*, ss 56 and 57 of the (Saskatchewan) *Evidence Act*; and, s 34.1(5),(5.1) of the (Ontario) *Evidence Act*.

distinguished from their records systems. Such practice has created a case law that ignores the technology that produces the records, and it contradicts the Evidence Acts' admissibility requirement for proof of "the integrity of the electronic documents system by or in which the electronic document was recorded or stored."[78]

The quality of electronic records management has these effects upon the cost and effectiveness of discovery proceedings:

(1) bad records management can prevent accessing all relevant electronic records in the form in which they were created (one's own creations) or stored (received records);
(2) an unnecessary increase in the time and expense needed to bring an ERMS up to sufficient quality to ensure all relevant records are retrieved; and therefore,
(3) the need to inquire into the state of an opponent's ERMS with questions such as: (a) "Is your client's electronic records management system in compliance with the National Standards of Canada for electronic records management?";[79] (b) "When was the last time an expert in electronic records management certified your client's electronic records management system as being in compliance?"; and (c) "What alterations have been made to your client's records management system during the time that the records in question have been recorded or stored?"

Such questions are necessary because of: (1) the complete dependence of an electronic record upon its ERMS for everything that it is and can be used for; and (2) the information needed to be produced to have an adequate evidentiary law for records. A party may try to avoid the high cost of bringing an ERMS up to standard by claiming that the discovery demands made by an opponent are "disproportionate" to what is in dispute. That assertion could be supported by a technical report from a records management expert, which no lawyer or judge at present has sufficient knowledge of ERMS technology to challenge. As a result, the party with bad records management will not have to make production of records that may be helpful to an opponent, but the party having good records management will easily make production of all records in its possession, including records that may hurt that party's position. Similarly, rulings of admissibility will have an unacceptably high probability of being wrong if made in the absence of evidence as to the state of "system integrity."

Compare: if the evidence of an alleged expert witness is not tested by examination of the expert's qualifications, the damage caused by relying on that evidence will not be known. The same danger is present if the quality of records management is ignored.[80] The beginning of the kind of examination of an ERMS

---

[78] *Ibid*. Most of the Evidence Acts use the word "record" instead of "document" in their electronic records provisions (as does the *Canada Evidence Act*'s electronic records provisions, ss 31.1-31.8). However, the business record provisions in s 30 of the *Canada Evidence Act* use "record."

[79] *Supra* note 7.

appropriate to electronic discovery proceedings is exemplified in *Siemens Canada Ltd. v. Sapient Canada Inc.*[81] An application was brought: (a) to impose a discovery plan on the parties, setting out *inter alia* the scope of documentary discovery and the custodians whose documents should be searched; (b) for a further and better affidavit of documents from the defendant; and (c) for timely production of documents not already produced by the defendant. In response, the defendant applied, in the event that the plaintiff was successful on its motion, for an order for further documentary production in regard to named executives of the plaintiff. The decision of the Court Master stated:

> [156] I am prepared as a consequence of the foregoing analysis to grant portions of the relief sought by Siemens. I am therefore directing that Sapient undertake:
>
> (a) Further back-up tape restoration at or around June 29, 2009 for the 10 original custodians and for the custodians identified in these reasons;
> (b) Application of the original Sapient search terms to the complete .pst files of all such custodians (rather than self-selection);
> (c) De-duping of that collection against the documents already reviewed by Sapient and/or produced by Siemens; and
> (d) An application of a relevancy definition for the purposes of manual review to take into account issues and problems with the progress of the Project in earlier years.
>
> [157] Sapient's cross-motion is Dismissed.

This decision shows why a procedure is necessary to end the time-consuming and expensive applications practice that plagues electronic discovery proceedings (see the next section).

A similar, albeit much more modest and simple example of the need for evidence as to the records system that produces the evidence in question is

---

[80] For example, the decision in *Zenex Enterprises Ltd. v. Pioneer Balloon Canada Ltd., supra* note 21, in effect holds that the state of a party's ERMS is irrelevant to electronic discovery proceedings. Specifically, it holds that the parties are not to demand to know how searches for relevant records were conducted, nor can they investigate parts of an opposing party's ERMS, such as hard drives. This ignores the fact that the accessibility and storage of electronic records are essential parts of ERMS technology. Because an electronic record is but an electronic impression on an electronic storage device, it is dependent upon its ERMS for everything that it is and can be used for. Therefore, using an electronic record without inquiring into the state of records management of its ERMS is like using an expert witness without inquiring into the qualifications of that expert. And therefore, electronic discovery cannot produce fair and accurate results unless the quality of the parties' electronic records management is investigated, particularly so its compliance with the National Standards of Canada for electronic records management (*supra* note 7).

[81] *Siemens Canada Ltd. v. Sapient Canada Inc* 2014 ONSC 2314, 2014 CarswellOnt 5280, [2014] O.J. No. 1930 (Ont. S.C.J. [Commercial List]).

provided by *R. c. Soh*.[82] The Court accepted the need to receive evidence on the issue of admissibility as to how the computer system that produced the "electronic documents" worked. The evidence concerned printouts and screen photos of a saved Facebook conversation between the complainant and the accused the day after an alleged sexual assault. The complainant testified as to how she accessed her Facebook account and how the system worked. The evidence was admitted as electronic documents under the electronic document provisions of the *Canada Evidence Act*, sections 31.1-31.8.[83]

The principles of ERMS technology set out in the National Standards of Canada[84] for electronic records management provide an authoritative basis and structure for such inquiries during electronic discovery and admissibility proceedings, but they have almost no presence in the case law. Using electronic records as evidence is an example of using a new technology without the regulatory framework that prevents that technology from causing injury, damage, and inadequate decisions from the courts. The reply "but we have had no trouble before," makes necessary the rebuttal "that is because you have never been adequately challenged before." Supposedly, if a lawyer were sued by a losing client for inadequate discovery or other form of investigation necessary for obtaining information as to the winning party's records system's ability to produce all relevant records, that lawyer would have a successful defence by proving that he did all that the law allows.[85]

---

[82] *R. c. Soh* 2014 NBQB 20, 2014 CarswellNB 69, 2014 CarswellNB 70, [2014] N.B.J. No. 41 (N.B. Q.B.) at paras 20-32. This is a criminal case, but almost all that is stated herein is applicable to criminal proceedings. A rare recognition of the need to apply the national standards was the basis of the decision in, *R. v. Oler*, 2014 ABPC 130, 2014 CarswellAlta 1042, [2014] A.J. No. 669 (Alta. Prov. Ct.). It dealt with the disclosure and admissibility of maintenance and other records concerning the Intoxilyzer 5000C, in relation to charges of impaired driving and "over 80" (ss 253(1)(a) and 253(1)(b) of the *Criminal Code*, *supra* note 17). *Supra* note 29 and accompanying text, and *R. v. M. (C.)*, 2012 ABPC 139, 2012 CarswellAlta 996 (Alta. Prov. Ct.) at paras 47-55. See also: Ken Chasse, "Electronic Records as Evidence", online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438350> and other relevant articles at: <http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1398484>.

[83] *CEA*, *supra* note 2.

[84] *Supra* note 7.

[85] The article, "Inadequate Investigation/Discovery Now the #1 Cause of Claims" (3 June 2013) *Slaw* (blog), online: <http://www.slaw.ca/2013/06/03/inadequate-investigation-discovery-now-the-1-cause-of-claims-2/>, by Dan Pinnington, the Vice President Claims Prevention and Stakeholder Relations at LAWPRO, the legal profession's insurer in Ontario, states that inadequate discovery and investigation by lawyers is the number one cause of claims against the insurer. That is a good indication of the damage caused by the inadequacy of the law that controls the scope of the issues relevant to electronic discovery proceedings. Clients must accept the consequences of the high probability of an opponent's making an inadequate production of documents. The full article, "Take the Time to Get it Right," is presented in the August 2012 edition of LAWPRO magazine (vol. 11, no. 3). A PDF copy is accessible online: <http://www.practicepro.ca/LawPROmag/Inadequate_Investigation_Claims.pdf>.

## VIII. THE NECESSARY LEGAL INFRASTRUCTURE FOR A FORMAL PROCEDURE FOR CERTIFYING COMPLIANCE WITH THE NATIONAL STANDARDS OF CANADA FOR ELECTRONIC RECORDS MANAGEMENT

The legal profession should be advising clients who have ERMSs that are not small to have them certified by experts in records management at least once per year, so as to be in compliance with Canada's National Standards for electronic records management. That should be a routine part of electronic records management, as should certification of compliance immediately after any significant change to an ERMS such as mergers and acquisitions making necessary the melding of two ERMSs into one or any reorganization or creation of an ERMS. Then, failure to produce such certification, or other evidence as to compliance, should raise a rebuttable presumption of inadequate production on discovery, and inadmissibility of electronic records as evidence. Proof of compliance could also be made by other evidence, such as that of a records manager. Whatever the chosen method, compliance with the national standards must always be proved.[86]

By means of such certification, issues concerning compliance with the national standards could be dealt with quickly by a simple exchange of certificates of compliance. The onus of proof would thereby be placed upon the possessor of the ERMS, rather than upon an opponent to show that the other party's records management has caused inadequate production on discovery, and an inability to satisfy the requirements of admissibility. With a small exception, the case law stands against giving such access to an opposing party's ERMS or part thereof.[87] In comparison, we all have to have our motor vehicles checked for safety and polluting emissions. Large ERMSs produce an equally important and voluminous "traffic." A proactive system of compliance is necessary. The present reactive system for complaints takes no account of the dangers and defects described above. Because parties who suspect that inadequate production of documents has occurred do not have access to an opponent's ERMS, a complaints method of enforcing adequate discovery is inadequate.

Two of the four records management components for such a certification process are already in place: (1) Canada has authoritative national standards for electronic records management, which are based upon well established international standards;[88] and (2) there is a well developed profession of

---

[86] *Supra* note 7.

[87] The case law may give access to a third party expert to look for particular documents or to check a hard-drive (hard drive), a computer, or a database, but not to check the state of overall electronic records management. It isn't asked for and the *Sedona Canada Principles* text doesn't deal with it; *supra* notes 32-34 and accompanying texts. Nor does the case law allow information as to how searches for records were done, even though searches may be inadequate due to bad records management. See for example *Zenex Enterprises Ltd. v. Pioneer Balloon Canada Ltd.*, *supra* notes 21 and 80.

[88] *Supra* note 7.

experienced experts in ERMS technology. The other two can easily be put in place: (3) a procedure whereby the Canadian General Standards Board, being the sponsor of the national standards, can licence such experts individually as being competent to provide certifications of compliance with the national standards; and (4) a standard form of certificate, placed in the national standards, for certifying compliance with them. Such certification of compliance work has been done for many years by experts in electronic records management. And to induce such certifications to become a routine practice, a subsection would be added to the electronic records provisions of the Evidence Acts making proof of the compliance of an ERMS with the National Standards of electronic records management—proof of the "integrity" of the ERMS, sufficient to achieve the admissibility of its records.[89]

For many years I have participated in such work with ERMS experts. Often it is only such certification of compliance that clients seek, particularly so when a regulatory agency or other official requires it, but only a small percentage of certifications are thus compelled, and in turn, voluntary certifications involve but a small percentage of the organizations that should obtain them. Such low levels of formal compliance are reinforced by the courts' avoidance of issues as to the state of ERMS management. It is a practice that should and would be reversed if the electronic records provisions of the Evidence Acts contained a rebuttable presumption of inadequacy of records for discovery and admissibility, in the absence of such certification of compliance. The "evidence to the contrary" rebuttal allowed by such presumptions could be provided by the "evidence of compliance" of the manager of the ERMS in question. However provided, proof of compliance with the national standards must be a necessary part of discovery, and a condition-precedent to admissibility. Or, the amendment could state that proof of the "integrity" of an ERMS can be made by proving compliance with the national standards. See the Appendix for suggested amendments to sections 30 and 31.1-31.8 of the *Canada Evidence Act*.

As a result, records management law would be much speeded on its way to becoming a recognized and major field of the practice of law, as would be the necessary close association with the work of experts in ERMS technology. Only then would the law provide an adequate legal infrastructure regulating the consequences of the fact that an electronic record is completely dependent upon its ERMS for everything. A law that is so heavily based upon a technology cannot ignore the exact nature of that technology if it is to provide "justice." The present application and practice of Canada's laws as to the discovery and admissibility of electronic records do not.

Therefore, if proof of compliance is to make electronic discovery and admissibility proceedings adequately respectful and inclusive of the ERMS technology upon which they are based, it needs the formalization, recognition, and authority of law. An example as to how that is to be achieved is provided by

---

[89] See the text accompanying note 97 in the Appendix.

section 5 in Part 1, Division 1 of PIPEDA.[90] That "Protection of Personal Information" Division makes mandatory compliance with the "principles set out in the national standard of Canada entitled, Model Code for the Protection of Personal Information, CAN/CSA-Q830-96," in Schedule 1. A similar relationship in law should be expressly established between electronic discovery and admissibility proceedings, and the National Standards of Canada for electronic records management, *i.e.*, the Evidence Act rebuttable presumption, or at least a subsection stating that proof of compliance is one of the ways of achieving the admissibility of electronic records as evidence (see the Appendix below). That alone would make information as to the state of compliance a necessary part of electronic discovery proceedings.

The development of such legal infrastructure is necessary given: (1) the dependence of every legal service upon electronic records; (2) electronic records are the most frequently used kind of evidence; and (3) other widely used areas of the law such as privacy and access to information, electronic commerce, taxation, and criminal law, are dependent upon electronic records. Technology needs legal infrastructure, and legal infrastructure needs lawyers. Therefore, lawyers must be cognisant of the technology underlying the laws in regard to which they provide legal services. The present practice concerning electronic discovery and admissibility of electronic records is not.

If the innovations suggested above are implemented, litigation will not be available only to "rich" people and institutions. The purposes of these innovations are to: (1) enforce compliance with the national standards for electronic records management; (2) solve the high cost of the "review" stage of electronic discovery proceedings; (3) create a law-based simple and affordable procedure by which proof of compliance with the national standards can be made in litigation proceedings; and (4) to establish the "records management lawyer" as a specialist and make that a support service available to all other lawyers.

## IX. THE NEED FOR A CERTIFIED SPECIALTY THAT IS "RECORDS MANAGEMENT LAW"

In 2011, I applied to the Certified Specialist Board of the Law Society of Upper Canada (Ontario) to recognize "records management law" as an area of specialized practice. My application was refused. A letter from the Board, dated October 3, 2012, states in part: "the Board has determined that your proposal does not disclose a sufficient number of lawyers practising in this field, which is a prerequisite to the establishment of a new area of specialization. . . . The Board has suggested that Records Management Law may fit into a broader specialty area of Information Technology, which would capture an established practice area representing a larger number of practitioners."

---

[90] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

The necessary reply is: the designation of areas of the practice of law as specialties (areas of formally designated specialization) should be based upon public need, not the number of lawyers asking for such designation, without independent verification of public need. In other words, such licensing boards should be enabled to be proactive and not merely reactive.[91]

However, I do think "Information Technology" as an area of specialization is a good stepping stone to the necessary populating of "records management law" with lawyers. In the interim, however, "information technology law" will be perceived as a rather vague designation as to its scope. I suggest that it have the following three divisions: (a) privacy and access to information; (b) electronic commerce; and (c) records management law. But the "records management lawyer," designated as a specialist, is needed now to give such specialty the necessary formalization, recognition, and authority of law, for the reasons set out herein.

In summary, the principle reasons for recognizing that "records management law" will have to be a major area of the practice of law are:

1. Expertise to assist other major areas of the law (in addition to electronic discovery) that are dependent upon electronic records such as: admissibility proceedings concerning records adduced as evidence; privacy and access to information; electronic commerce; criminal law; and taxation.[92] These other areas already have their certified specialist practitioners, which alone provides sufficient justification for recognizing "records management law" as a specialized area of the practice of law.
2. Due to every electronic communication, electronic service, and formal activity producing an electronic record, all areas of the law are now dependent upon ERMS technology, and therefore all lawyers should be prepared to deal with ERMSs and electronic records technology, or be able to obtain expert assistance, and in regard to every legal service be able to cope with the greater number of records made available by that technology.

---

[91] For example, the solution to the "access to justice-unaffordable legal services problem" is to create specialized services for those parts of each type of legal service that lawyers find that they cannot do cost-efficiently and profitably. The higher degree of specialization and scaled-up volume of production beyond what exists in private practice will produce economies of scale that no law firm can match. Legal research is one such area, which is why most often it is given to law students to do. This "cutting costs by cutting competence" strategy should be replaced by the support-services strategy that is based upon increasing competence by increased specialization and producing a much greater cost-saving by greatly scaled-up volumes of production. See for example Ken Chasse, "The Technology of Centralized Legal Research Can Solve the Unaffordable Legal Services Problem" (2 August 2014), online: < http://papers.ssrn.com/sol3/papers.cfm?abstract_id = 2475350 > .

[92] A beginning to this specialized practice is the appointment of electronic discovery experts by larger law firms, *supra* note 66.

3. Assistance in making legal services available at reasonable cost: the availability of such expertise as a support service to all law offices would make such services available much more cost-efficiently than they could otherwise be provided.
4. The creation of such a certified specialty would be of considerable assistance in making the "review" stage of electronic discovery proceedings affordable (in the ways described above).
5. Such certified specialists would make law firms more attractive to potential corporate investors in law firms (assuming that legislation regulating law societies is amended to allow law firms to become investment properties).[93]
6. Such certified specialists would be better able to work with providers of related non-legal services concerning ERMS technology and working with law firms, as recommended, for example, for consultation by the Professional Regulation Committee's Report of Feb. 27, 2014, of the Law Society of Upper Canada (LSUC).[94]

## X. CONCLUSION

The innovations advocated in this article are:

(1) the use of the National Standards of Canada for electronic records management to provide the definition and principles necessary for the effective and cost-efficient operation of the electronic records provisions in the Evidence Acts in Canada (their "*integrity* of the electronic records system" test of admissibility), instead of that need for a definition being ignored;
(2) the creation of a simple and cost-efficient certification process for proof of compliance with those national standards, which process would facilitate such use of the national standards;
(3) changing the strategy for reducing the cost of electronic discovery and admissibility proceedings, from a "cutting costs by cutting competence" strategy—the competence of the law to provide accurate results—to a

---

[93] See this statement by the LSUCs: "The Law Society released Alternative Business Structures and the Legal Profession in Ontario: A Discussion Paper on September 24, 2014, to seek input from lawyers, paralegals, stakeholders and the public about Alternative Business Structures (ABS)", online: < http://www.lsuc.on.ca/ABS/ > . And see the Feb. 27, 2014 Report to Convocation by LSUC's Professional Regulation Committee, online: < http://goo.gl/P0YKx3 > . (The Law Society of Upper Canada has retained its title as created in 1797, while Ontario was still the British colony of Upper Canada (being further up the St. Lawrence River than Lower Canada (Québec).) See the executive summary, (at the top of page 1444, in the materials for Convocation's meeting of Feb. 27th; the Report begins at p 1438). These recommendations are more fully developed in paras 162-179, at pp 1495-1499, being pages 49-53 of the Report itself).

[94] *Supra* note 65 and accompanying text.

strategy that does not deny the nature and dangers of the technology upon which such proceedings are based;

(4) a method for reducing the cost of the "review" stage of electronic discovery proceedings, *i.e.*, the indexing of all significant client records so that accessing and reviewing records for relevance and privilege can be done as one operation, and done with the speed of electronic searching;

(5) increasing the ability of the law to render accurate and just results by use of the "triangle of interdependent concepts" for the use of electronic records as evidence.[95] Its purpose is to maximize the efficacy of the "triangle of interdependent proceedings."[96]

(6) revising the records provisions of the Evidence Acts in Canada in support of these innovations by adding a "rebuttable presumption of inadequacy," so as to enforce proof of compliance with the National Standards of Canada for electronic records management;

(7) the creation of the "records management lawyer" specialist, necessary for implementing the field of "records management law" as a means of controlling the costs of litigation;

(8) amending sections 30 and 31.1-31.8 of the *Canada Evidence Act*, as suggested in the Appendix below, to facilitate these innovations.

These innovations are necessary: (1) to give electronic records and their ERMS technology an adequate legal infrastructure for litigation and other legal services; and (2) to make litigation that is dependent upon the use of records available at reasonable cost.

---

[95] *Supra* notes 25-28 and accompanying text.

[96] See above, immediately after the paragraph containing notes 25-27.

# APPENDIX

## Amending sections 30 and ss. 31.1 to 31.8 of the *Canada Evidence Act* (CEA)

Sections 30 and 31.1 to 31.8 of the *Canada Evidence Act* should be amended so as to:

(1) remove any doubt that section 30 can deal with hearsay issues concerning all records—both electronic records and non-electronic records;
(2) section 30 can expressly use sections 31.1 to 31.8 *CEA* to provide the standard for judging the admissibility of electronic records;
(3) establish their complete interdependence;
(4) nullify the argument that section 30 cannot deal with electronic records because it was enacted in 1969, which was before the present electronic records technology existed;
(5) facilitate corresponding amendments to be made to the provincial and territorial Evidence Acts so to bring about uniform wordings and the compatibility of all the Evidence Acts in Canada (excluding the corresponding provisions in Book 7 of the Civil Code of Québec);
(6) bring about a greater use of the case law among all jurisdictions by removing such differences in legislation.

**Therefore:**

1. End the best evidence rule by removing the reference to it in section 31.2(1) *CEA*. It was created when copies were hand-written, thus creating an issue as to the accuracy of the copying from the original. Now, all records obtained from digital (electronic) storage are "originals." But if in fact any record were hand-copied or otherwise contrived to be presented as an "original," the amendments below would provide the necessary protective tests.
2. Change the word "documents" in sections 31.1 to 31.8 to "records." Section 30 uses "records," and so should sections 31.1 to 31.8, particularly so as to link section 30 to them as recommended herein.
3. Replace the present section 31.2 with this section:

> s. 31.2 Anyone seeking to admit an electronic record as evidence:
>
> (1) has the burden of proving the integrity of the electronic records system by or in which the electronic record was recorded or stored;
> (2) proof of the integrity of an electronic records system may be made by proving compliance of the system with the national standard of Canada, *Electronic Records as Documentary Evidence* CAN/CGSB-72.34-2005;[97]

---

[97] This national standard encompasses all ERMSs, including those devoted to imaging and microfilming purposes. However, 72.11, *supra* note 7, remains the industry standard for imaging.

(3) in the absence of evidence to the contrary, an electronic record satisfies subsection (1) if it has been manifestly or consistently acted on, relied upon, or used as a record of the information recorded or stored in it.

4. Amend section 31.5 by adding the words, "Subject to s. 31.2, . . . ."
5. Remove section 31.3. Subsection 31.3(a) would be unnecessary because of s. 31.2(2), and subsections 31.3(b) and (c) should be removed because they enable the use of an electronic record that cannot satisfy the requirements of subsection 31.2 as amended above.
6. Replace the present section 30(1) with this subsection:

> 30(1) Where oral evidence in respect of a matter would be admissible in a legal proceeding:
>
> (a) the admissibility of an electronic record that contains information in respect of that matter is established on proof of the requirements of s. 31.2;
> (b) the admissibility of a record that is not an electronic record that contains information in respect of that matter is established by proving that neither the source of the information that it contains nor the method or circumstances of its preparation indicate a lack of trustworthiness.

7. Restrict section 30(6) to non-electronic records, and to issues concerning "weight" (probative value).
8. Remove the words, "made in the usual and ordinary course of business" from subsection 30(2) so that it begins: "Where a record does not contain information in respect of a matter . . . ."
9. Where necessary, the definition provisions would have to be changed accordingly.