ARTICLE:

WHY A LEGAL OPINION IS NECESSARY FOR ELECTRONIC RECORDS MANAGEMENT SYSTEMS

By **Ken Chasse, J.D., LL.M.**

A legal opinion as to compliance with the law and with standards for electronic records management

The law now judges the reliability of an electronically-produced record by judging the reliability of the electronic records system it comes from.[1] That means that a record is no better than the quality of the records system in which it is recorded or stored. Proof of the integrity of an electronic record requires proof of the integrity of the electronic records system. Therefore, to be able to present records that will be accepted in legal proceedings, or in response to any formal demand for records and information, an organization's records management system must comply with the law that specifies the quality requirement. Any changes made to a records system that might affect the record system's quality or level of performance should be accompanied by a legal opinion. That opinion will aim to assure that:

1. There exists no reason in law why the organization's records should not be accepted in legal proceedings, and by all legal authorities; an opinion by a lawyer cannot guarantee that records will definitely be accepted as evidence, because there are important performance requirements and decisions that have to be made, such as: (a) the quality of the evidence and argument used in attempting to get the records accepted as reliable evidence; (b) the quality of the testimony used in support; and (c) the quality of the decision-making by the judge or head of the tribunal making the decision. These are variables that the lawyer giving the legal opinion cannot control. Therefore a legal opinion can go no further than to indicate that there exists no reason in law why the client's records should not be accepted as evidence.

2. The organization's records system is in compliance with the law.

3. Its records system is in compliance with authoritative standards for electronic records management such as for example, the National Standards of Canada for electronic records management, or if appropriate, the standards of International Organization for Standardization in Geneva, Switzerland (the ISO).[2] The National Standards of Canada for electronic records management are *Electronic Records as Documentary Evidence* CAN/CGSB 72.34-2005 (72.34), summarized in appendix B; and *Microfilm and Electronic Images as Documentary Evidence* CAN/CGSB-72.11-93 (72.11)

1 *For example, section 34.1(5), (5.1) of the Evidence Act (Ontario), R.S.O 1990, E.23 (OEA), and ss. 31.2(1) of the Canada Evidence Act, R.S.C. 1085, c. C-5 (CEA), require for an electronically-produced record (an 'electronic record') to be admissible evidence, proof of the integrity of the electronic records system by or in which the record is recorded or stored. Twelve of Canada's 14 jurisdictions have such provisions in their Evidence Acts or comparable legislation. British Columbia and Newfoundland and Labrador are the two jurisdictions that do not yet have such legislation. However, because it is the use of electronic technology and not the law that makes all electronic records dependent upon their records systems for their reliability and integrity, it is argued that all jurisdictions everywhere must analyze the quality of a record's records system in order to determine whether that record is reliable.*

2 *http://www.iso.org/iso/iso_catalogue.htm.*

(updated in 2000).[3] These two standards, and the law of Canada, are used as examples in this article because of the author's familiarity with them. The provisions of the Evidence Acts expressly make relevant the use of such standards in determining the admissibility of electronic records, for which see s. 34.1 OEA, and s. 31.5 CEA. The standards 72.34 and 72.11 require that 'an organization shall always be prepared to produce its records as evidence'.[4] If an organization cannot satisfy this and all of the requirements of the National Standards, it must provide a good reason as to why its records should not be accepted for any legal purpose.

Supporting legal authorities are provided in the footnotes, but the body of this text is written for clients, potential clients, and their records managers. Canadian laws and electronic records management standards are used as examples of comparable texts operative in most jurisdictions.[5]

However, the nature of electronic records should dictate the contents of the laws and standards that regulate electronic records management, and not the converse. That is because of the difference between an electronic record and a paper record – a paper record has an existence apart from its records management system; an electronic record does not. It follows that it is a serious error to conclude that it is not necessary to be concerned with the authoritative standards of electronic records management. Even where local laws do not incorporate the 'system integrity' concept, together with the other principles of the standards that reflect the reality that an electronic record is dependent for everything upon the state of its electronic records system, it is necessary for the lawyer to be aware of the 'system integrity' concept.

More than general knowledge of law and records management is required

Such legal opinion would be part of a report written by those having special knowledge and experience in records management, and in the law of records management – both fields must be involved. This is a highly specialized area requiring more than merely general knowledge of records management and of the law.

The work of a records manager should not include legal advice

Often organizations will choose to have only records management work done in improving their electronic records management systems, without an accompanying legal opinion. The records management specialist that is hired will provide at best, general legal information, and may state that the records system appears to be in compliance with the law, but then add words to the effect that 'this is not a legal opinion.' Such a response presents two serious weaknesses: (1) the organization itself must take responsibility for any loss suffered by knowingly relying on legal information given by an unqualified person; and (2) the records management expert may have given what amounts to a legal opinion. Legal information may be worded so as to invite the client to rely upon it to the extent of foregoing the advice of a lawyer. Therefore, by stating that a document is not a legal opinion does not mean that it is not one, or that it is not the giving of legal advice. Where a records management expert provides such an opinion, it could be in violation of the law by providing legal services without being licensed to do so.[6] Any client who knowingly contracted for and accepted such work, are arguably complicit in any violation of the law. It is conceivable that the cost-saving in not obtaining

3 *CAN/CGSB-72.34-2005 is the designation in Canada's National Standards System, which states that it is standard 72.34 (its short form reference) developed by the Canadian General Standards Board (the CGSB), and approved and publicly proclaimed in December 2005 to be a National Standard of Canada by the Standards Council of Canada, the coordinating body of the System. National Standards of Canada are written by agencies that develop standards accredited by the Standards Council of Canada. Draft standards are submitted to the Council for its approval, and then published by the development agency. The Council's function is to ensure that the formal, established process for developing standards has been followed. On acceptance by the Council, they become National Standards of Canada. These standards are the work of committees composed of experts from the records and information management field, including legal advisors. They have been recognized by the ISO, the International Organization for Standardization in Geneva, Switzerland. The CGSB is a government agency within Public Works and Government Services Canada, and has been accredited by the Standards Council of Canada as a national standards-development organization. The process by which such national standards are created and maintained in Canada is described within the Standard itself and on the CGSB's web site at http://www.techstreet.com (under 'Standards Development').*

4 *72.34, subsection 5.4.3(c), p. 17.*

5 *See Stephen Mason, general editor, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010); Stephen Mason, editor, International Electronic Evidence (British Institute of International and Comparative Law, 2008).*

6 *For example, in the province of Ontario, sections 26.1 and 26.2 of the Law Society Act, R.S.O. 1990, c. L.8, establish the offence and penalty for, practising law or providing legal services by one who is not a lawyer (a person who is not licensed to practice law).*

proper legal advice may lead to substantial costs, including inadequate preparation for and performance in litigation.

Why it is necessary for records management work to be conducted in the light of legal advice

The most frequent reasons why organizations choose to have records management work done to their records systems without accompanying legal advice are:

1. such has always been the practice;
2. only records management work is to be done, not legal work;
3. the previous law required only that records management be carried out in accordance with 'good business practice' and there seems no reason to change;
4. there has been no trouble in the past;
5. few understand that electronic technology has changed not only records management, but also the laws that apply to electronic records and electronic records management – particularly the laws as to using records as evidence; and,
6. the organization has their own legal department.

None of these reasons justifies the failure to obtain appropriate legal advice. Records and information management is a specialized area of the law. If records managers believe that they have not needed legal advice before, it is because they and their records systems have not been challenged before. The law has substantially changed since 2000, and there are now national and international standards for electronic records management. Therefore, dealing with records management in accordance with good business practice is no longer sufficient. For example, records might not be accepted as evidence in legal proceedings and by government regulatory authorities if the practice that is followed is not of sufficient quality to comply with such standards.

Records management by good business practice is no longer enough

Before electronic records management systems, there were paper records systems. The law judged the reliability of a record for all legal purposes by its history, and not by the quality of the records system it came from. Such pre-electronic record systems, when operated in accordance with good business practice, appeared to provide a good history to each record. A legal opinion was not considered necessary. The changes in the law have changed this.

The change that required legislation dealing with records management was not the introduction of electronic technology to paper records management, as happened when mainframe computers processed data from paper records, beginning in the late 1950s. The management of paper records was made more efficient and productive, but not fundamentally different. Rather, the important innovation that changed the law was the creation of electronic records management systems. Electronic records management systems separated data and information from their traditional media of storage, paper and microfilm. When a record is but a group of electrons in an electronic records system, or photons of light in an optical records system, and not created on a piece of paper or microfilm, it is completely dependent upon the state of its records system for its existence, accessibility, and integrity. As a result of the transition in technology, new standards of records management were required, as well as new laws.

To comply with the law, records management must conform to objective, principle-based, authoritative national and international standards, and no longer act in accordance with personalized, subjective opinions as to what good business practice might be (the business and records management phrase), and, 'the usual and ordinary course of business' (the Canadian lawyer's phrase taken from the Evidence Acts in Canada).

The 'system integrity test' – records management based on 'systems' concepts, not 'records' concepts

Electronic technology has made this simple difference, but one of great consequence – it has separated information (data) from the media upon which it is stored. This means a record is a flow of electrons in an electronic

records system (or photons of light in an optical system), or an electronic impression on a storage device. It follows that the electronic record relies on the technology, and the record is potentially vulnerable to every piece of software, hardware, communications device and system, and records management practice and procedure that is part of the electronic records management system. The electronic record is also vulnerable to the dangers of the internet – every type of malicious software, and electronic intervention (such as hacking) that may be launched at it from anywhere in the world. The law provides that for records to be admissible in evidence, proof is required of the integrity of the electronic record system in which it is recorded or stored. For instance, the Canada Evidence Act provides:

31.2 (1) The best evidence rule in respect of an electronic document is satisfied

(a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or

(b) if an evidentiary presumption established under section 31.4 applies.

The worth of an electronic record is dependent upon proof of the integrity of the electronic record system in which it is recorded or stored. This is referred to as the 'system integrity test' for the acceptance of electronic records in legal proceedings.

A paper record in a file folder, in a file drawer, has a physical existence separate from its records management system. An electronic record does not. Paper records and electronic records are very different things, having very different vulnerabilities. The law, and records management, have to reflect that difference. When requesting advice about records management practice, the difference should be reflected in the nature of the advice sought.

Records not accepted as evidence make the organization vulnerable

An organization that does not have its records accepted as evidence in legal proceedings cannot assert or defend its rights and property and the obligations owed to it. Even if records are accepted as evidence, they may be considered to have little weight (credibility, probative value, persuasiveness), because the records system they come from might not comply with the recognized standards of electronic records management. It therefore follows that electronic records may be of little use to the organization as evidence in legal proceedings.

An electronic records management system is not an isolated stand-alone system

A paper record system is a stand-alone unit. It is not physically connected to other records systems. To damage a single record or a number of records, it is necessary to have physical access. But an electronic record system is connected to the electronic world by the internet. If not properly secured, electronic records will be vulnerable to all of the malevolence of the virtual world. This is why security is one of the many subjects dealt with by standards, such as the National Standards of Canada. All electronic record management systems are dependent upon the quality of their software, hardware, and records management policies.

Records management in accordance with a regime of legal compliance is necessary

To have the benefits of electronic technology as applied to records management, it is necessary to have a more complex and sophisticated type of records management process in place that reflects appropriate legal knowledge and experience. For instance, legal advice concerning electronic records management requires expertise in those laws that make demands upon electronic records systems. Those are: the laws of evidence for legal proceedings; the laws of electronic commerce; the personal information protection and privacy laws; and the laws of electronic discovery. The legislation is highly interrelated and interdependent in the concepts they use and the requirements they impose. They apply to all electronic records systems. In addition, there are the records management requirements of taxing agencies such as those of the Canada Revenue Agency, and the requirements of the national and international standards for electronic records management. Every new law that is dependent for its proper operation upon high quality records management, imposes an additional set of requirements upon an organization's electronic records management. The result is that electronic records management is subject to a regime of legal compliance. Compliance with good business practice is no longer enough.

Previously, undertaking records management in accordance with good business practice took care of the legal requirements (except for specialized records requirements for specialized industries and services). Now, new electronic technology and new laws are dictating the nature and requirements for electronic records management.

Whenever alterations to a records system are made that are more than minor changes, a legal opinion should be obtained that certifies that the records system complies with the relevant standards for electronic records management. Failure to do so means that records managers fail to comply with the 'prime directive' of the National Standards of Canada for electronic records management: 'an organization shall always be prepared to produce its records as evidence.'[7] Without complying with such standards, there is little probability of electronic records being accepted as evidence. That might mean losing the protection of the law.

Records have not been challenged before

Often records managers will indicate that because they have never had difficulties in the past, there is no need to consider taking legal advice from a lawyer that specializes in the law of records management. They are generally correct: their records and records systems have not usually been challenged before. But this state of affairs will change. Challenges to records managers will become frequent when lawyers obtain advice from records managers about how to cross-examine as to the state of records management and compliance with its standards The law concerning records management has to be monitored. Lawyers are now beginning to challenge software and are beginning to demand the production of source code.[8] It contains information as to the developmental history of each software program.[9] Software is the foundation of an electronic records management system. If its 'error rate' is too high, it will be deemed to be unreliable, and so will the records systems that depend upon it.[10] Lawyers are becoming aware of the national and international standards for electronic records management referred to above. The standards contain basic, but detailed principles and practices that can be used to cross-examine records managers who have to defend their records systems. A records system that is shown not to be in compliance with the records management and legal requirements of these standards might be deemed to be unable to satisfy the requirements of the Evidence Acts and other legislation related to the use of records. If a records system cannot satisfy the records management requirements established by these national and international standards of records management, it is questionable whether anyone should rely on its records.

If good records management is not thought to be an important factor in maintaining competence and competitiveness, it will suffer in the event of litigation, because although business most often relies on active and recently created records, litigation much more often relies on older, inactive, and retired records. To obtain access to all such relevant records, and do so in a cost-efficient manner, requires good records management, especially to cope with the challenges presented by the electronic discovery process.

Standards compliance

The National Standards of Canada for Electronic Records Management

Government departments are aware of the National Standards of Canada for electronic records management. Organizations that receive government funding have been requested to obtain professional certification that their records systems comply with them. These standards can now be considered to authoritative because:

1. they have been created by a national standards-writing body, the Canadian General Standards Board (a federal government agency), that has been recognized as such by the Standards Council of Canada;

7 72.34, clause 5.4.3c (p. 17).

8 Source code contains programming techniques and is essential documentation in the development of software. It is a record of that development. Therefore, to evaluate software, it is necessary to produce the source code.

9 There has been considerable American litigation challenging source code, particularly in regard to Intoxilyzer, Breathalyzer, and Alcotest machines (used in impaired and drunk driving cases), and therefore 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 (no longer available on-line), and Charles Short, 'Guilt by Machine: The Problem of Source Code Discovery in Florida DUI Prosecutions,' 61 Fla. L. Rev. 177 (January, 2009); also see State of New Jersey v. Chun 194 N.J. 54; 943 A.2d 114; 2008 N.J. LEXIS 133 (S.C.N.J., 2008), USSC certiorari denied by Chun v. N.J., 2008 U.S. LEXIS 6506 (U.S., Oct. 6, 2008); State of Minnesota v. Underdahl and Brunner 2009 Minn. LEXIS 178 (S.C.Minn., April 30, 2009).

10 As to the whether there should be a presumption as to a computer system being in proper working order at all materials times, see the discussion in Chapter 5, 'Mechanical Instruments: the presumption of being in order', in Stephen Mason, gen ed, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010).

2. they have been recognized and accepted by the Standards Council of Canada, which means that they have been declared to be National Standards of Canada;

3. they incorporate as normative references the standards of the International Organization for Standardization (ISO), which means that Canada's national standards comply with international standards, which means in turn, that Canada's standards, its electronic records, and its electronic records management should be accepted everywhere;[11]

4. they are relevant to the interpretation and application of the electronic records provisions of the Evidence Acts – relevant to legal proceedings of all kinds, and to the use of records as evidence;

5. they are used as authoritative references by authors of books and articles concerning records management; and,

6. they are recognized as authoritative by agencies of Canada's federal and provincial governments.

Electronic records are like drops of water in a pool of water – 'system integrity' and vulnerability to the internet

Electronic records are not like paper records, but rather like drops of water in a pool of water. We cannot define or describe an electronic record in an electronic record system by describing the history of a particular group of electrons, no more than we can describe the history of a drop of water after it falls into a pool of water. When drops of water later emerge from the pool of water, we cannot associate any of them with particular drops that entered the pool of water. This simile illustrates the critical difference between paper records management and electronic records management. A paper record maintains its physical existence and identity while stored in its file or folder. The reliability of a paper record can be proved by proving its particular history from its creation until it is submitted as evidence in a court, quite apart from the reliability of its record system. But an electronic record does not maintain its existence as a particular group of electrons in its records system, no more than a drop of water maintains its existence and identity in a pool of water. The molecules of the drop of water are subject to everything that happens to the pool of water. To prove the fate of any drop of water requires proof of what has happened to the pool of water: the purity of any drop in the pool of water requires proof of the purity of the pool of water as a whole. Similarly, once an electronic record is entered into an electronic records system, it is subject to everything that happens to that electronic record system and can possibly happen to that system, including its compliance with records management standards, security, and vulnerability to the internet.

It follows that proof of the integrity of an electronic record requires proof of the integrity of the electronic records system. That is what the electronic records provisions of the Evidence Acts in Canada require – proof of the 'integrity of electronic records system in which the record is recorded or stored.' Unlike a paper record, an electronic record is no better than the records system in which it is recorded or stored. There is no valid argument that proving the system integrity of an electronic record requires merely proof of the system integrity of that part of the records system in which the record existed – every record and its records system are part of the same, single electronic 'pool.' However, if parts of an organization's records operations are sufficiently independent in operation, management, structure, and purpose, such parts may each constitute an 'electronic records system' for purposes of proving system integrity, and therefore the acceptability of any particular electronic record as evidence. It follows that there is no valid argument that the system integrity test as to what is acceptable evidence is unworkable, because it requires proof of the integrity of all of an organization's local, national or international records management operations in order to use a single print-out as evidence.

The major areas of law concerning records management — 'legal compliance' will become more complex and the legal profession's duty with it

In addition to the laws of evidence that determine whether records will be accepted as evidence in legal proceedings,

11 *Canada' s national standards for electronic records management incorporate the ISO' s standards as normative references. For example the national standard, Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005, and the summary in appendix B. Clause 2.1 (p. 2) states: ' The following referenced documents are indispensible for the application of this document.' Clause 2.6 (pp. 3-4) contains the list of ISO standards that Canada' s national standards for electronic records management are based upon.*

the major areas of law concerning records and records management systems include: electronic commerce; personal information protection and privacy; and electronic discovery in legal proceedings. The electronic commerce legislation enables electronic information and communications to have the same status in law as statements paper documents.[12] It uses the same concept of 'proof of the integrity of the records system' that is the foundation concept of the electronic records provisions of the Evidence Acts. For example, s. 8(1)(a) of the province of Ontario's Electronic Commerce Act, 2000 S.O. 2000, c. 17, states that an electronic record can serve as an original document if 'there exists a reliable assurance as to the integrity of the information contained in the electronic record… .' This use of the concept of the 'integrity of the information' is very similar to the 'system integrity test' of the electronic record provisions of the Evidence Acts. Therefore this legislation is very interrelated and interdependent, one Act with the other. Electronic records used in commerce must be able to be used as evidence in legal proceedings, otherwise the organization's legal and financial foundations cannot be protected. Therefore, two of the most important functions of an organization in protecting its rights under the law – evidence for legal proceedings and electronic communications for commerce – are dependent upon the reliability and the integrity of its electronic records system.

The personal information protection and privacy laws impose requirements on all organizations to protect the personal information of all persons within the organization.[13] Therefore such legislation imposes an additional set of requirements upon electronic records management.

Electronic discovery is the mandatory process by which the opposing parties to legal proceedings exchange relevant records before and in preparation for trial. In order to reduce the time and cost of trials, the opposing lawyers are required to exchange all relevant records in their possession. An organization, perhaps because of faulty records management, may not know the extent of its records holdings, and may not be able to produce records because they remain recorded on old technology that can no longer be viewed. The law of electronic discovery has become voluminous and complex in both Canada and the U.S.[14]

Taken together, the four areas of the law, along with the records requirements of tax legislation and those of the national standards of records management, impose a regime of legal compliance upon electronic records management. In addition, many industries and fields of business and government activity are subject to their own specialized legislation that imposes specific records management requirements.

An important recent example of how the law is failing to comprehend the increasing complexity of technology and how it is used, lies in the 'proportionality' concept of electronic discovery.[15] As currently explained and applied, the concept of proportionality has arguably been developed without any investigation of the nature of an electronic record, in particular how it and its records management systems differ from traditional paper records systems. In addition, it was devised without regard as to how technical developments such as cloud computing and offshore outsourcing of records management functions increase the vulnerability of electronic discovery to cheating – to using sophisticated and complex electronic records management to prevent effective and fair electronic discovery.

12 *For example, Ontario' s Electronic Commerce Act, 2000, S.O. 2000, c. 17; the Consumer Protection Act, 2002, S.O. 2002, c. 30, Schedule A, ss. 37-40 (internet agreements); Alberta' s Electronic Transaction Act, S.A. 2001, c. E-5.5; British Columbia' s Electronic Transactions Act, S.B.C. 2001, c. 10; and, Part 2 of the federal Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. This legislation allows, with some exceptions, the use of electronic alternatives to paper for recording or communicating information or transactions. The source for this legislation is the Uniform Electronic Commerce Act (UECA), a model Act produced by the Uniform Law Conference of Canada in 1999. In Quebec, the Act to Establish a Legal Framework for Information Technology, R.S.Q. 2001, c. C-1.1, does not follow the UECA model. The Criminal Code R.S.C. 1985, c. C-46, as amended, ss. 841 to 847, provides for ' electronic commerce' in regard to electronic court documents.*

13 *For example, the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Part 1, which is a federal statute that is also applicable to provinces, such as Ontario, that have not enacted their own PIPA (personal information protection Act) – see s. 26(2)(b). Alberta, British Columbia, and Quebec have done so; see: Alberta' s Personal Information Protection Act, S.A. 2003, c. P-6.5, and British Columbia' s Personal Information Protection Act, S.B.C. 2003, c. 63.*

14 *In Canada, electronic discovery in civil court proceedings is dominated by the three Sedona Canada texts (available from the Sedona Canada Working Group 7 site): The Sedona Canada Principles— Addressing Electronic Discovery, on-line: The Sedona Conference, Canada, January 2008; E-Discovery Canada web site, hosted by LexUM (at the University of Montreal), available on-line at http://www.lexum.umontreal.ca/e-discovery.*

15 *The Sedona Canada Commentary on Proportionality in Electronic Disclosure and Discovery (October, 2010); The Sedona Canada Commentary on Practical Approaches for Cost Containment—Best Practices for Managing the Preservation, Collection, Processing, Review & Analysis of Electronically Stored Information (April, 2011); 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, and the other articles cited therein.*

The common defects found in electronic records management systems

The list in appendix A provides a number of defects commonly found in the records systems of a wide variety of well established and managed organizations. A single effect, or groups of such defects will cause an organization to have its records fail to protect its legal rights, obligations, and property. For this reason it is imperative for organizations to take appropriate legal advice on such matters.

A lawyer knowledgeable and experienced in records management law is required

Sometimes records managers decide that because their organizations have a legal department, they do not need outside special legal advice. It is true that any competent lawyer, given enough time and study, could give an opinion to serve all of the complex requirements of electronic records management. But that would not be a cost-efficient use of that lawyer's time, whose expertise and area of legal practice lie in other areas of the law. A records manager should always consult the organization's legal department before deciding that the legal advice of a lawyer is not needed for a records management project, or that the legal department can provide the legal advice.

A lawyer who attempts to give a legal opinion or legal information in regard to the law of records management has to have detailed knowledge of all the legislation, court decisions, text books, published articles, authoritative guidelines and reports, concerning:

1. the laws of evidence relating to the use of records as evidence in legal proceedings before courts and tribunals (agencies, authorities, boards, and commissions);

2. the laws of electronic commerce; personal information protection and privacy; electronic discovery; and taxation related to electronic records;

3. authoritative standards such as those of the ISO and the National Standards of Canada concerning electronic records management;

4. specialized laws that apply to each client's industry or area of business or government activity;

5. developments in the laws of the United States of America on these subjects, because they often provide early warning of new laws and legal problems and possible solutions.

Records managers are no longer competent to be able to fully understand the complexity of the law. It follows that an organization's records manager who decides that a legal opinion is not necessary in regard to changes made to, or in preparation for audits of its electronic records system, is taking on an unjustifiable risk – a substantial risk of a failed audit, and of not having the organization's records accepted as evidence in legal proceedings.

Ken Chasse is a Barrister and Solicitor, Toronto, Canada. He has been a records management lawyer for over 35 years, providing opinions and advice concerning the use of records in legal proceedings, compliance with laws relating to privacy, electronic commerce, taxation, and national and international standards of electronic records management.

kchasse@fixy.org

Appendix A

The common defects of records management systems that affect admissibility and weight

The following serious defects in electronic records management systems are common, even in the best of organizations. Each can diminish the 'system integrity' of the whole system such that its records might not be accepted as evidence. Among the most common defects, frequently found in the systems of large organizations, including those of government departments and agencies, universities, utilities, and commercial organizations are the following:[16]

1. the extent of the records holdings is not known;
2. records are neither properly classified nor indexed such that the retrieval of records relevant to any particular subject is very difficult if not impossible;
3. no definitive classification system among institutional, transitory, and personal records (e.g., determining which research and business records are those of each professor, and which are those of the university);
4. no records manual, or one that is not kept current, or is not complied with;
5. no bylaws (or orders of comparable authority from senior management) dealing with the records system – essential for establishing an organization's 'usual and ordinary course of business' in regard to its records system;
6. e-mail is not classified, indexed nor pruned, or possibly not retained; there is no e-mail protocol operative throughout the organization;
7. records repositories are not well defined nor centrally accessible;
8. 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;
9. original paper records are not disposed of after being put into digital storage in a secure records management environment (with the exception of industry, professional, or special legal requirements as to retaining designated originals);
10. 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;
11. 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; for instance there can be extensive duplicates and an inability to track official or original versions;
12. no audit trails or controls providing relevant information about deletions, such as, when, who, by what retention destruction or disposal authority;
13. no clear definition and practice as to what is meant by the deletion of a record such that records may or may not continue to exist in back-up storage, thus diminishing knowledge of the extent of records holdings and their control;
14. changes in technology result in unaccounted for and undocumented changes in records practice;
15. no consistent practice as to other forms of communication that create records, e.g., video and audio recordings, instant messaging, mobile telephone communications;
16. no retention and disposal programme for records lifecycles;
17. years after a merger or acquisition, the records system is still operating according to the conflicting rules of its component parts;
18. no chief records officer with clearly defined and adequate authority;
19. 'orphaned data,' that is, records that can no longer be retrieved or read because the new technology that now operates the records system is incompatible

16 *This list of defects comes from the records management experts the author works with on projects concerning the maintenance, alteration, upgrading, and updating of large electronic records systems. The most frequent type of such projects concern analyzing records management systems for compliance with the National Standards of Canada for electronic records management, 72.34 and 72.11. The analysis and recommendations by which to achieve compliance are incorporated in a report that has both a records management and 'legal compliance' part.*

with the old technology that created those records (a migration program should accompany the installation of new technology);

20. poor security protection;[17]

21. inadequate compliance with the records management requirements of the personal information protection and privacy laws,[18]

22. inadequate testing, auditing, and quality control;

23. substantial failure to comply with the National Standards of Canada concerning electronic records management, and a lack of appreciation of the consequences of failing to comply.

There is also an important 'auditing consequence' for defective records systems. An auditor or accountant, when testing the internal controls of a records system, may find that they cannot be relied upon. Then the audit cannot be conducted using a 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 per cent verification. If cross-examination of a records manager revealed that no reliance could be placed on the system and that a full substantive audit had to be undertaken, that in itself would give significant support to an argument that the records from that records system should not be relied upon. The records system would lack system integrity. Therefore the system integrity test of the electronic records provisions of the Evidence Acts has a strong similarity to auditing standards.

Such defects could result in these losses: (1) the system integrity test for the acceptance (admissibility) of records as evidence in legal proceedings not being satisfied; (2) the demands of electronic discovery might be inadequately complied with; and (3) the credibility of the electronic records system's records will be damaged (a record's 'weight' (credibility) as evidence will have been lowered). For example, because of such defects, a disclosure request as simple as, 'produce all records on subject X,' cannot be complied with, with complete certainty as to the accuracy, comprehensiveness, and knowledge of the time, cost, and disruption to be incurred in fulfilling such request. A records management system should be regularly audited internally, and periodically independently, externally audited.

An electronic records system having the above defects cannot comply with the prime directive of the national standards, which is: 'An organization shall always be prepared to produce its records as evidence.'[19] In turn, it cannot comply with the system integrity test by which the admissibility of electronic records is to be determined. Where a party fails to comply, it will risk having to overcome a strong presumption of a lack of system integrity, and therefore a strong possibility that their records not being accepted as evidence in legal proceedings.

The credibility of any part of a record system can be decisively damaged by defects in its other parts – 'decisively', meaning the inadmissibility of any of its records when adduced as evidence, that is courts refusing to accept records because their record systems are unreliable. The system integrity test of the electronic record provisions[20] determines the admissibility of an electronic record by judging the integrity of the complete electronic records system, not just any particular

17 The ninth point of proof specified in the National Standard of Canada, Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005, section 5.5 states:
i) security – security procedures are in place to protect the integrity of the records management system; at least the following should be able to be proved:
1. protection against unauthorized access to data and permanent records;
2. processing verification of data and information in records;
3. safeguarding of communications lines;
4. maintenance of backup copies of records to replace falsified, lost and destroyed permanent or temporary records;
5. retention and disposition of electronic records in compliance with legislated and internal retention periods and disposition [disposal] requirements, and documenting such compliance and disposition schedules; and,
6. a business continuity plan for electronic records and associated data, including off-site copies of essential files, operating and application software [a 'disaster recovery' factor].

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

19 Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005, clause 5.4.3 c) at p. 17; and, Microfilm and Electronic Images as Documentary Evidence CAN/CGSB-72.11-93, paragraph 4.1.2 at p. 21.

20 For example, s. 34.1(5),(5.1) of the Ontario Evidence Act (OEA); s. 41.4(1),(2) of the Alberta Evidence Act (AEA); s. 23D of the Nova Scotia Evidence Act (NSEA); and, s. 31.2(1)(a) of the Canada Evidence Act (CEA).

part. However, those provisions also invite the use of recognized standards to help to determine admissibility.[21] Therefore in Canada, the National Standards of Canada, Electronic Records As Documentary Evidence CAN/CGSB 72.34, and Microfilm and Electronic Images as Documentary Evidence CAN/CGSB 72.11-93 must be applied. They provide rules and procedures for records management with which to satisfy the tests and the undefined phrases in the Evidence Acts in Canada. They are based upon the systems concept of electronic records management, as distinguished from the records concept of paper records management.

As a truly objective test, the 'system integrity' test should mean that a record system either has that essential integrity or it does not. A test is to be applied to the whole of a records system, not just to those parts of it concerned with particular records. The interpretation of the test does not allow for admissibility obtained by proving the integrity of only a particular part of a record system, even if the contents of a record adduced as evidence were directly affected by only a part. The test being a system test, there can be no valid argument that the sub-standard quality of other parts of the records management system not directly related to the production of the records in question are irrelevant. Doubt cast upon a part casts doubt upon the whole. That will be the strategy for opposing the use of records as evidence – exploit a defect in any part of the records management system to defeat the records adduced from any other part of the system. Like the credibility of a witness as to sincerity, and character in general, the 'system integrity' of a records management system is viewed as a whole.

Therefore, the definition as to what a 'system' is, is critical to admissibility (the acceptance of records as evidence). If an organization has many electronic records systems, each separate 'system' will have to comply with all of the requirements of the applicable records management standards. Therefore it might facilitate the admissibility of records to operate the specialized records management functions as each constituting a separate records management system. Deciding the scope, jurisdiction, and function of a records management system can be a complex question of fact and law. Given the complex world wide web of records management system connections and communications, court decisions determining whether a particular record is the product of one more records management systems will increase in number and complexity.

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

But, given the great capacity and flexibility of movement and manipulation provided by electronic records management (this term is used in its widest sense to include optical and other digitized systems of manipulating and creating records), electronic records must be judged by the practice and reputation of the records management system they come from and not simply by their own history, as was sufficient prior to the addition of the electronic record provisions to the Evidence Acts. In addition to the electronic record provisions, the federal, provincial, and territorial Evidence Acts in Canada also contain business record provisions, (for example, s. 30 CEA, 35 OEA, s. 42 BCEA, and s. 23 NSEA). They require proof that a record was made, 'in the usual and ordinary course of business.' For electronic business records to be admissible evidence in legal proceedings, both sets of provisions must be satisfied. The Evidence Acts of Alberta and Newfoundland and Labrador do not contain business record provisions, and therefore admissibility is determined under the business records exception to the hearsay rule at common law; which in Canada is defined by the decision of the Supreme Court of Canada in *Ares v. Venner* [1970] S.C.R. 608, 12 C.R.N.S. 349, 14 D.L.R. (3d) 4, (S.C.C.). The Evidence Acts of British Columbia and Newfoundland and Labrador do not contain electronic record provisions. Therefore the requirements for electronic business records would be determined under business record provisions of British Columbia (s. 42 of the British Columbia Evidence Act),

21 *For example, s. 41.6 AEA, s. 23F NSEA, s. 34.1(8) OEA; and, s. 31.5 CEA. Without such reference to the national standards, the use of the vague word 'integrity,' would be difficult to apply.*

and under the common law rule in Newfoundland and Labrador. Neither was intended to deal with electronic business records, nor are they drafted suitably for electronically technology as it is applied to records management today. Quebec does not have an Evidence Act as such, but it has comparable provisions in its Civil Code of Quebec, L.R.Q., c. C-1991, Book Seven, 'Evidence,' particularly: articles 2831-2842, 2859-2862, and 2869-2874, and in An Act to Establish a Legal Framework for Information Technology, R.S.Q., c. C-1.1, ss. 2 and 68.

And apart from the needs of litigation, the same applies to the requirements of all legislation dependent upon high quality records management, such as legislation concerning electronic commerce,[22] personal information protection and privacy,[23] electronic discovery,[24] and the records requirements of government departments and agencies.[25] A failure to satisfy the requirements of one will probably mean, and signal, a failure to satisfy all. Sharing a common electronic records management foundation, they have a close interdependence and consequent probability of failure.

The alternative interpretation of the 'system integrity' test, that it need be satisfied only in relation to those parts of an electronic records system that affected the records adduced as evidence and not all parts of the system is impractical. The operative concept is 'system integrity', not, 'the system integrity of the relevant part.' Data can too easily and unaccountably be moved throughout a system. It is not possible to know what future litigation will demand of a records system, which means it is dangerous as well as impractical to leave the maintenance and updating of a system, or a part of it, until particular records are required as evidence. Alterations made in contemplation of litigation undermine the credibility of the entire system. They raise an inference that the system lacked the necessary integrity before such alterations. Also, such alterations and the records they produce would not be made 'in the usual and ordinary course of business,' as required by the business record provisions of the Evidence Acts.[26] Therefore such alterations would most likely result in a failure to satisfy both the electronic record and business record provisions of the Evidence Acts. That is one of the reasons why 'the Prime Directive' of the National Standards of Canada states, 'an organization should always be prepared to produce its records as evidence.'[27] Compliance with 'the Prime Directive' is a substantial part of compliance with the whole of the National Standards of Canada.

However, specialized parts of an electronic records management system may be sufficiently independent as to constitute separate 'systems' for purposes of the system integrity test and the use of records as evidence. Therefore, it is not necessary to prove the integrity of the whole of an organization's local, provincial, national, and international records management operations in order to use a single print-out as evidence.

Appendix B

A brief summary of electronic records management system compliance standards established by the National Standard of Canada, Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005 (72.34).[28]

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

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

24 *For example, Ontario 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."'*

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

26 *Section 30 of Canada Evidence Act, and s.35 of the Ontario Evidence Act. All provincial and territorial Evidence Acts have such business record provisions except for the Evidence Acts of Alberta and Newfoundland and Labrador.*

27 *Clause 5.4.3c of, Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005 (p. 17); and, paragraph 4.1.2 of, Microfilm and Electronic Images as Documentary Evidence CAN/CGSB-72.11-93 p. 21).*

28 *Only 72.34 is summarized, because it is comprehensive of all electronic records, including those of the other National Standard of Canada 72.11, Microfilm and Electronic Images as Documentary Evidence, supra note 3. However, 72.11 is still the ' industry standard' for the records management requirements of imaging.*

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

1. Management authorization and accountability: to test that records and document management receives authoritative recognition from senior management. [5.4.3] This is an essential aspect of a RM (records management) system's 'system integrity,' and 'usual and ordinary course of business,' which are requirements of the Evidence Acts.

2. Documentation: to test whether sufficiently detailed and unambiguous documentation exists for the procedures used to manage records and documents; that this documentation is sufficiently known to all parties that have access to modify the electronic records in any manner; and that the guidance in this documentation is followed by all such parties at all times.

3. Reliability: Reliability of electronic records is tested according to the following legal rules:

   Authenticity: to test whether records and documents actually come only from the person, organization or other legal entity asserting to be their author or authorizing authority. [5.2.2]

   Integrity: the electronic records provisions of the Evidence Acts state that where any such record is challenged as to whether it is a reliable copy of its electronic source, such challenge is satisfied by 'evidence of the integrity of its electronic records system by or in which the data was recorded or stored.' Therefore, proof of the integrity of any particular electronic record is established by proof of the integrity of the electronic RM system that recorded or stored it – this is the 'system integrity test' of admissibility for electronic records (the acceptability of records in legal proceedings). [5.2.3] To aid proof of such 'system integrity,' the electronic records provisions of the Evidence Acts provide three presumptions that are paraphrased in subsections of the national standard [5.2.3 (a), (b), (c)].

4. The procedures manual and corporate records officer:[29] to test whether there is a current manual covering all policies, procedures, and systems in regard to all records and information management. Authorization, accountability, and documentation for such a manual, and for the creation of the position of corporate records officer should be based upon a bylaw, or order of similar authority within the organization. There can be one or more manuals covering these functions. [5.4.2; 5.4.3]

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

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

7. Retention and Disposal: to test that an appropriate retention program has been documented and is followed. RM policy should provide guidelines for records storage, protection, and retention so that records remain available and usable as required for decision-making, program-service delivery, and accountability. Disposal should occur in accordance

29 *72.34 uses the term 'corporate records officer' (CRO), instead of 'chief records officer,' or, 'chief records manager.' In section 3 of 72.34, 'Terms and definitions,' is this definition (p. 6): '3.17 corporate records officer CRO, [the] organization Person authorized to act on behalf of the organization and entrusted for overall governance of the electronic record management program and related programs.'*

after business, legal, and audit requirements have been served and the applicable retention periods have expired, such disposal being formally documented. [6.8; 6.9]

8. Back-up and system recovery: to test whether appropriate back-up procedures are in place and maintained. [6.10]

9. Security and protection: to test whether appropriate security is in place and is maintained. [6.12]

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

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

12. Additional tests that touch on related areas such as system management, workflow, and version control. [8; Annexes A, and C]1

