2010

Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later

Luciana Duranti

Corinne M. Rogers

Anthony F. Sheppard
Allard School of Law at the University of British Columbia, sheppard@allard.ubc.ca

Citation Details

Luciana Duranti, Corinne Rogers & Anthony Sheppard, "Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later" (2010) 70 Archivaria 95.

Electronic Records and the Law of Evidence in Canada: The *Uniform Electronic Evidence Act* Twelve Years Later

LUCIANA DURANTI, CORINNE ROGERS, and ANTHONY SHEPPARD

RÉSUMÉ Cet article analyse la pertinence du *Uniform Electronic Evidence Act*, douze ans après son adoption, pour traiter de la complexité des documents créés, consultés ou conservés dans un environnement numérique. Face aux changements rapides dans le domaine de la technologie, les auteurs croient qu'on ne peut pas tenir compte de la nature et des caractéristiques des documents numériques en effectuant de simples modifications à la loi existante, mais qu'on doit faire promulguer une nouvelle législation qui tiendra compte de la collaboration étroite entre les professionnels qui travaillent dans les domaines des documents d'archives, du droit et du respect de la loi, et des technologies de l'information. Les nouveaux règlements, couvrant l'ensemble des questions liées à la pertinence, l'admissibilité et le poids de la preuve documentaire électronique, devront être basés à la fois sur le corpus du savoir de chaque profession, les résultats de la recherche interdisciplinaire et les normes existantes par rapport aux documents d'archives. La promulgation de tels règlements aiderait les tribunaux à tirer des conclusions exactes, basées sur des documents numériques créés dans des environnements fiables et conservés sous forme authentique aussi longtemps que nécessaire, ce qui amoindrirait la confusion continue au sujet de l'admissibilité et de l'usage des documents numériques dans les procès.

ABSTRACT This article analyzes the adequacy of The *Uniform Electronic Evidence Act,* twelve years after its adoption, in dealing with the complexity of the records created, used, or stored in the digital environment. In the face of rapidly changing technology, the authors believe that the nature and characteristics of electronic records cannot be accounted for by simple modifications to the existing law of evidence, but require a new enactment following upon a close collaboration among records professions, legal and law enforcement professions, and the information technology profession. The new rules, comprehensively encompassing issues of relevance, admissibility, and weight of electronic documentary evidence, must be based on the body of knowledge of each profession, on the findings of interdisciplinary research, and on existing records-related standards. The enactment of such rules would help the courts make accurate findings of fact, based on electronic records that are created in a reliable environment and preserved in an authentic form for as long as they might be needed, and would alleviate ongoing confusion about the admissibility and use of electronic records in litigation.

ARCHIVARIA 70 (Fall 2010): 95–124

Introduction

> The very sanctity of the place demonstrates the inviolability of archives, for they used to be in temples … Nor have archives ceased to be inviolate even though today they are not in temples. Rightly, says Ulpian, do we call inviolate those things which are neither sacred nor profane, but confirmed with a certain inviolability. What is supported by a certain sanctity, that is inviolate though it be not consecrated to God. Marcianus also says that is inviolate which is protected and fortified against injury by man … Therefore, even now it is permissible to call archives inviolate … In agreement … are Bartholus, Baldus, Alexander, Jason, Castrensis and other interpreters of civil law everywhere in the Authentica *ad haec*, in the Codex, "On the Reliability of Instruments.
>
> — Baldassare Bonifacio, 1632[1]

As argued by Bonifacio in his treatise about archives, Roman jurisprudence, as well as Roman law and, later, canon law, considered records, regardless of their age or antiquity, as implicitly trustworthy, not only because they were kept in inviolable places, but also because they were under the shield of "skilled and painstaking men" called by various names, such as "archivists (*archivista*) … custodians (*custos*) … keepers of the chests (*scriniarius*)." As a consequence of their inviolate nature, records were regarded as "useful for instructing and teaching men … for clearing up and illustrating obscure matters …for conserving patrimonies and thrones, all things public and private … as much better than navy yards, as much more efficacious than munitions factories, as it is finer to win by reason rather than by violence, by right rather than by wrong."[2]

In the twelfth and thirteen centuries, Roman law spread throughout Europe as the *Jus Commune* or common law, which remained as the foundation of the *Jus Singulare* or individual law of each country. Given the credibility attributed by the *Jus Commune* to records, forgery became a widespread problem, to the point that specific rules had to be introduced to prevent it, such as a requirement of great formality in the creation and structuring of the original record, and a requirement of authentication by experts whenever a record was offered as proof of a fact at issue. This adaptation of the law to the circumstances of the times is at the root of the two basic rules of evidence at common law: 1) the best evidence rule, which requires that an original record be submitted as evidence whenever possible, and 2) the authentication rule, which requires that either direct or circumstantial evidence be presented that a record submitted as evidence of a fact at issue is what it purports to be.[3]

1 Lester K. Born, "Baldassare Bonifacio and His Essay *De Archivis*," *The American Archivist*, vol. IV, no. 4 (October 1941), p. 236.

2 Ibid., p. 234.

3 Heather MacNeil, *Trusting Records: Legal, Historical, and Diplomatic Perspectives*

However, it was only in response to the doctrinal conflicts of the Reformation and Counter Reformation of the seventeenth century that a systematic method was developed to determine the authenticity of records. The publication of *De Re Diplomatica* in 1681 – the treatise by Dom Jean Mabillon that provided the tools for assessing the conformity of a record's elements of form to established procedures, thereby establishing its authenticity[4] – supported the philosophy of rationalist empiricism, and paved the way for the development of the concept of evidence as inference[5] and for exceptions to another basic rule of evidence at common law, the hearsay rule. According to this rule, documents offered as evidence are hearsay as they contain assertions made outside a court of law. However, on the grounds of necessity (absence of other available evidence) and circumstantial probability of trustworthiness, records, that is, documents made or received in the course of business and kept for the needs of such business, could be considered admissible, because the process of their creation made them more likely to be reliable, unless the opposing litigant showed the contrary.[6]

By the nineteenth century, business records were regarded by common law rules of evidence as likely to be reliable if they also complied with the best evidence and the authentication rules. Today, the legal rules governing the use of documentary evidence, although several times refined and extended, are very similar to those established at the end of the nineteenth century. These rules have always been of direct interest to records professionals responsible for the creation and maintenance of records for obvious reasons, while they have not usually concerned those responsible for the long-term preservation of records, primarily because their responsibilities did not extend to a direct involvement with the first part of the records life cycle, and did not have an impact on the form and integrity of the records through time. This situation changed as soon as archivists became involved with electronic records.[7]

It is a fact established by research and experience that we cannot preserve electronic records, but only our capacity to reproduce them time after time,

(Dordrecht, 2000), p. 3. For a discussion of common law versus civil law, see pp. 32–35.

4 See Luciana Duranti, "Diplomatics: New Uses for an Old Science," *Archivaria* 28 (Summer 1989), pp. 7–27.

5 See MacNeil, *Trusting Records*, pp. 20–24.

6 See John Henry Wigmore, *Evidence in Trials at Common Law*, 11 vols. (Boston, 1972–1983; rev. 1974), Vol. 5, para. 1632.

7 The ability to preserve reliable and authentic electronic records depends on the circumstances of their creation and maintenance, requiring archivists (trusted custodians) to advise on matters related to those processes, and records managers to understand the implications of record creation and maintenance for long-term preservation. See Yvette Hackett, "Methods of Appraisal and Preservation," in *International Research on Permanent Authentic Records In Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, eds. Luciana Duranti and Randy Preston (Padova, 2008), available at http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_19.pdf (accessed on 18 October 2009).

in a continuing effort to beat technological obsolescence.[8] The nature of electronic records challenges traditional rules of evidence and procedure, and requires their reformulation. For example, the traditional best evidence rule is no longer relevant because of the absence of an original in the digital environment. The authentication rule also is inadequate, because it cannot be established that an electronic record is the same as its first instantiation simply by looking at the record itself, but it is necessary to refer to an unbroken line of traces left by all those who interacted with the record or to the legitimate custody of a professional who can account for them.[9] Furthermore, the complexity and variety of digital information systems and the often uncontrolled ways in which they are used, make it difficult to identify records within them and the business activities to which they are linked, thereby challenging the application of the business records exception to the hearsay rule. Finally, ever-changing technology speeds up the obsolescence not only of earlier record-making processes, but also of the laws regulating admissibility.

Therefore, all records professionals responsible for creating, managing, maintaining, and preserving records inviolate over time are – or should be – very much concerned with what the law has to say about the admissibility and weight of electronic records. No one would question the responsibilities of managers of current records to maintain record-keeping systems that offer reliability, integrity, compliance, comprehensiveness, and systematization in order to create and maintain records that have integrity and are authentic, reliable, and useable. Archivists are also increasingly assuming responsibility for the unprecedented quantity and number of formats of digital material that could be introduced in litigation. The voices of records managers and archivists alike are needed to participate in the monitoring of existing rules and, if reform is needed, in the elaboration of new rules capable of supporting their efforts of protecting the trustworthiness of the records for as long as they exist.

The purpose of this article is to evaluate the *Uniform Electronic Evidence*

8 For example, see Luciana Duranti, Jim Suderman, and Malcolm Todd, "A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records," in *International Research*, eds. Duranti and Preston, Appendix 19, p. 1.

9 For a discussion of the characteristics of electronic records and their implication for the assessment of their authenticity see Heather MacNeil, "Providing Grounds for Trust: Developing Conceptual Requirements for the Long-term Preservation of Electronic Records," *Archivaria* 50 (Fall 2000), pp. 52–78, and Luciana Duranti and Kenneth Thibodeau, "The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES," *Archival Science*, vol. 6, no. 1 (2006), pp. 13–68, available at http://dx.doi.org/10.1007/s10502-006-9021-7 (accessed on 18 October 2009). See also Luciana Duranti, "From Digital Diplomatics to Digital Records Forensics," *Archivaria* 68 (Fall 2009), pp. 39–66.

Act, the 1998 Canadian legal system's statutory response to the growing use of digital technology as the primary means of conducting activities and producing records. We explore why the Act, now twelve years old, has not had a more significant impact on case law, despite still constituting the core of the Canadian law approach to digital documentary evidence.[10] We argue that the development of rules governing the ability of electronic records to be used as evidence throughout their life cycle depends on records that are reliable at creation, and that are maintained trustworthy and inviolate through time and over the long term. We believe that this requires close research collaboration not only between the records (records managers and archivists) and legal (lawyers, judges, notaries) professions, but also between these and the law enforcement and information technology professions, and that the conceptual and methodological body of knowledge of diplomatics, digital forensics, and archival science should guide such research.

Documentary Evidence – A Primer

The law of evidence, which still regulates proof in Canadian courts and tribunals, originated in England long before the computer and electronic recordkeeping. Ancient courts developed common law evidentiary rules to deal with the admissibility of hand-written parchment and paper records. In drawing these rules, and through subsequent reforms, the courts were careful to strike a balance between providing ease of proof of trustworthy records and avoiding, as much as possible, risks of fraud, forgery, and unreliability.

As the common law rules lagged behind developments in record-making and record-keeping practices, reforms began in earnest in the nineteenth century. They have continued ever since as the pace of technological advances accelerates. In the late twentieth century, computerization of commercial transactions and recordkeeping seemed to reformers to be so far ahead of the common law and statutory rules as to require more specific changes. Responding to these concerns, many jurisdictions enacted legislation to facilitate electronic transactions and recordkeeping so that electronic records could be admitted in proceedings as legal proof. These other jurisdictions adopted comprehensive provisions broadly regulating the admissibility and procedure governing computer evidence with updating amendments from time to time.[11] Diverging widely from these jurisdictions despite the similarity of

10 A discussion of the Act can also be found in MacNeil, *Trusting Records*, pp. 51–54.

11 See for example the Law Reform Commission of Western Australia, *Project No. 27, Part 1: Report on the Admissibility in Evidence of Computer Records and Other Documentary Statements* (Perth, 1980); Council of Europe, *Harmonization of Laws Relating to the Requirement of Written Proof and to the Admissibility of Reproductions of Documents and Recordings on Computers: Recommendation No. R (81) 20 Adopted by the Committee of*

our common law heritage and the problems to be addressed, the Uniform Law Conference of Canada (the major law reform agency in Canada [hereinafter ULCC]), took a minimalist approach to reform, and has not updated its initial provisions to meet the changing demands of technological advances. Whereas the other jurisdictions did not specifically deal with the best evidence and authentication rules in their broader reforms, the ULCC limited its narrower approach to those two rules. The need to keep law current with technological changes, especially in the areas of evidence and procedure, cannot be satisfied by legislation issued at a single point in time, but requires continuous and sustained updating.[12]

Even in the absence of legislation, some judges have expressed a willingness to admit new forms of evidence resulting from advances in technology, as long as their reliability was not disputed and they did not disrupt either the traditional roles of judge and jury, or court processes.[13] However, judges have also expressed a conservative point of view against initiating broad reforms of the common law rules of evidence to meet modern needs, preferring to encourage the legislatures to take on this sort of project.[14] Currently, the Supreme Court of Canada expresses a preference for confining the courts' role to initiating only "incremental" updating of the common law to meet changing times, leaving broader reforms of complex areas to the legislature.[15] Comprehensive and continuing reform of the procedural and

Ministers of the Council of Europe on 11 December 1981 and Explanatory Memorandum (Strasbourg, 1982); Queensland Law Reform Commission, *The Receipt of Evidence by Queensland Courts: Electronic Records, Issues Paper WP No. 52* (Brisbane, 1998).

12 See also Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep Up With Technological Change," *UNSWLRS* 21 (2007), available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/UNSWLRS/2007/21.html (accessed on 8 June 2010).

13 *R. v. Béland*, [1987] 2 S.C.R. 398, 43 D.L.R. (4th) 641, para. 20; *R. v. Nikolovski*, [1996] 3 S.C.R. 1197, 141 D.L.R. (4th) 647.

14 *Myers v. Director of Public Prosecutions*, [1965] A.C. 1001 (H.L), not followed in *Ares v. Venner*, [1970] S.C.R. 608, 14 D.L.R. (3d) 4.

15 *R. v. Salituro*, [1991] 3 S.C.R. 654, 1991 CanLII 59 (S.C.C.); *Grant v. Torstar*, [2009] 3 S.C.R. 640, 2009 SCC 61, para. 46; in *Watkins v. Olafson*, [1989] 2 S.C.R. 750, McLachlin J. (as she then was) for the court said: "Generally speaking, the judiciary is bound to apply the rules of law found in the legislation and in the precedents. Over time, the law in any given area may change; but the process of change is a slow and incremental one, based largely on the mechanism of extending an existing principle to new circumstances. While it may be that some judges are more activist than others, the courts have generally declined to introduce major and far-reaching changes in the rules hitherto accepted as governing the situation before them. There are sound reasons supporting this judicial reluctance to dramatically recast established rules of law. The court may not be in the best position to assess the deficiencies of the existing law, much less problems which may be associated with the changes it might make. The court has before it a single case; major changes in the law should be predicated on a wider view of how the rule will operate in the broad generality of cases. Moreover, the court may not be in a position to appreciate fully the economic and policy issues underlying the choice it is asked to make. Major changes to the law often involve devising subsidiary rules and procedures relevant

evidentiary aspects of digital records is a matter for legislatures, not for the courts.

In the common law tradition, proof of the facts at issue is sought through sworn oral testimony. If oral testimony is unavailable, records attesting to the facts may be offered as evidence in its place. Records, however, are considered a form of hearsay, and are technically inadmissible. This hearsay rule is overly restrictive, and, in practice, the inadmissibility of hearsay has been tempered at common law by certain exception rules and the "best evidence" rule. Exception rules depend on proof that the records submitted are reliable and necessary. Traditionally, the common law requirement of authentication asks a litigant offering a disputed paper record into evidence to preface its admissibility with foundation evidence, that is, with evidence external to the record identifying it as authentic and relating it to the issues in dispute. Usually a witness with personal knowledge of the record would fulfill such requirement by recognizing the record and explaining its relevance to the dispute. This requirement continues to apply to electronic records.

The common law best evidence rule required the litigant who sought to offer a record as proof of its contents to submit the original; however, if the original was unavailable for a legitimate reason, other means of proof of the contents of the (missing) original were acceptable. While the same witness who authenticated the record would usually be sufficiently knowledgeable to testify that it was the original, if the original were missing, the inquiry would turn to the legitimacy of the reason for its absence before other (secondary) evidence of its contents, such as the testimony of someone who had read the record, could be ruled admissible. Since at least the 1980s, Canadian courts have acknowledged that technological advances, such as photocopying and microfilming, eliminate the necessity of a strict observance of the best evidence rule.[16] Recent scholarship has eroded the application of the best evidence rule further, as it is recognized that the concept of original has lost its meaning for electronic records.

Another challenge recognized by the courts in receiving computer-generated or stored records derives from the fact that they may lack stability of form and content, and can be displayed on a variety of media, but it is not a bar to admissibility.[17]

---

to their implementation, a task which is better accomplished through consultation between courts and practitioners than by judicial decree. Finally, and perhaps most importantly, there is the long-established principle that in a constitutional democracy it is the legislature, as the elected branch of government, which should assume the major responsibility for law reform."

16 *Papalia v. R.*, [1979] 2 S.C.R. 256, 93 D.L.R. (3d) 161; *Kamloops Square Management Ltd. v. Baron*, [2006] BCCA 37, 51 B.C.L.R. (4th) 360, at para. 14–16; *Shanghai v. Mozaffarian*, [2002] BCCA 571, [2002] B.C.J. No. 216 (QL), at para. 22.

17 *R. v. Bell and Bruce*, [1982] 35 O.R. (2d) 65 C.C.C. (2d) 377 (C.A.), aff'd [1985] S.C.R. 287; *R. v. Lemay*, [2004] BCCA 604, 247 D.L.R. (4th) 470, at para. 33.

The *Uniform Electronic Evidence Act*[18]

The ULCC[19] comprises representatives of the federal, provincial and territorial governments of Canada, and various law reform agencies. It uses committees of experts to develop model legislation on various topics for possible adoption by the Parliament of Canada, and by the legislative assemblies of provinces and territories. In 1997, the ULCC adopted in principle the text of a proposed *Uniform Electronic Evidence Act* [hereinafter the UEEA, or the Act], and sought consultation prior to final approval.[20] At its next annual meeting, the ULCC officially adopted the UEEA[21] as a model legislation that proposed reform of the traditional common law evidentiary requirements for proof of authentication and best evidence, on the grounds that, while these rules worked well enough for paper records, they could not deal adequately with electronic ones.[22]

Most Canadian jurisdictions welcomed the UEEA's new approach to the admissibility of electronic records. In terms of general acceptance and implementation, the Act was a great success, and literally became uniform law across Canada, regulating the admissibility of electronic records offered into evidence in all criminal and most civil, quasi-criminal, and administrative proceedings. Four Canadian jurisdictions declined to adopt the UEEA: British Columbia, New Brunswick, Newfoundland and Labrador, and Quebec. New Brunswick and Quebec enacted distinctive provisions, which, however, do not apply to criminal proceedings.[23] Because the Canadian federal system confers legislative jurisdiction over criminal matters on the Parliament of Canada, the *Canada Evidence Act,* which includes the UEEA's provisions in sections 37.1–37.6, prevails in criminal proceedings anywhere in Canada, including provinces that did not adopt the Act for other types of proceedings within their jurisdiction. Even though British Columbia did not adopt it as such, the Act did influence provisions of the *British Columbia Evidence Act* relating to the requirements for proof for electronic court records.[24]

18 The text of the Act is reproduced for reference in the Appendix.

19 See http://www.ulcc.ca (accessed on 20 May 2010).

20 John Gregory, "*Canadian Uniform Electronic Evidence Act*," available at http://jya.com/eueea.htm (accessed on 20 May 2010).

21 *Uniform Electronic Evidence Act* (UEEA), available at http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2 (accessed on 20 May 2010)

22 For a discussion of the background to the UEEA, see Ken Chasse, "Electronic Records As Documentary Evidence," *Canadian Journal of Law and Technology*, vol. 6, no. 3 (November 2007), pp. 141–62, available at http://cjlt.dal.ca/vol6_no3 (accessed on 20 May 2010).

23 New Brunswick, *Evidence Act*, R.S.N.B. 1973, c. E-11, sections 47.1 and, 47.2; Quebec, *Civil Code of Quebec*, articles 2837–2840; and *An Act to Establish a Legal Framework for Information Technology*, R.S.Q. 2001, chapter C-1.1.

24 *Evidence Act*, R.S.B.C. 1996, c. 124, sections 41.1–41.4.

Jurisdictions chose to adopt the UEEA in one of two ways. Most legislatures, including the federal one, implemented the provisions of the UEEA by renumbering them and inserting them as amendments into their pre-existing evidence acts.[25] Two legislatures (PEI and the Yukon Territory) enacted the Act as a distinct statute, physically separate in the statute books from their evidence acts.[26] Regardless of which mode of implementation was adopted to determine the Act's physical location in the statute books, courts faced a common problem of statutory interpretation: how to reconcile the new provisions with the common law and statutory rules that already dealt with electronic records. In 2004, the Law Reform Commission of Saskatchewan (LRCS) expressed concern about problems that might arise because of lack of integration of the electronic records provisions with other evidentiary provisions.[27] For example, the electronic records requirements do not expressly refer to pre-existing rules for the admissibility of business records, rules that define them as including electronic records by using the phrase "any information that is recorded or stored by means of a device."[28] However, the LRCS did not regard the problems as sufficiently serious or practical to warrant amendments in the direction of integration.

Courts have reached diverse conclusions about the interface between existing evidentiary provisions and the new ones introduced by the Act. In *R. v. Bishop*,[29] the learned judge described the new rules as a "mini-code," implying that, as far as they went, they were complete and prevailed over other provisions, an interpretation that would maximize their impact. In contrast, in *R. v. Ganes*,[30] the learned judge held that existing provisions for admissibility of professional reports regarding licensing and signature regardless of form (as opposed to business records) prevailed over the new rules (which address requirements for authentication and best evidence). Electronic records,

25 Canada, *The Canada Evidence Act*, R.S.C. 1985, c. E-5, sections 31.1–31.8; Alberta, *Alberta Evidence Act*, R.S.A. 2000, c. A-18, sections 41.1–41.8; Manitoba, *The Manitoba Evidence Act,* R.S.M. 1987, c. E150, C.C.S.M. c. E150, sections 51.1–51.8; Ontario, *Evidence Act,* R.S.O. 1990, c. E.23, section 34.1; Northwest Territories, *Evidence Act*, R.S.N.W.T. 1988, c. E-8, section 37.1; Nova Scotia, *Evidence Act*, R.S.N.S. 1989, c. 154, sections 23A–23H; Nunavut, *Evidence Act*, R.S.N.W.T. 1988, c. E-8, section 37.1 as enacted for Nunavut pursuant to section 29 of the *Nunavut Act*, S.C. 1993, c. 28; Saskatchewan, *Evidence Act*, S.S. 2006, c. E-11.2, section 54.

26 Prince Edward Island, *Electronic Evidence Act*, R.S.P.E.I. 1988, c. E-4.3; Yukon Territory, *Electronic Evidence Act*, R.S.Y. 2002, c. 67.

27 Law Reform Commission of Saskatchewan (LRCS), Research Paper, *The Saskatchewan Evidence Act: A Review*, pp. 32–35, available at http://sklr.sasktelwebhosting.com/ (accessed on 20 May 2010). The paper refers to sections 29.1–29.6 of the previous *Evidence Act,* which were re-enacted in 2006 as section 54 of the current *Evidence Act*.

28 See for example *Canada Evidence Act*, subsection 30 (12); *B.C. Evidence Act*, subsection 42(1), *Manitoba Evidence Act*, subsection 49(1); and *Ontario Evidence Act*, subsection 35(1).

29 *R. v. Bishop*, [2007] ONCJ 441, at para. 30.

30 *R. v. Ganes*, [2005] S.J. No. 832 (Prov. Ct.).

according to the learned judge, were only admissible if they complied with the requirements of existing provisions, an interpretation that would minimize the effect of the new requirements.[31]

The merits of the UEEA have also received recognition outside Canada. For example, the Commonwealth Secretariat acknowledged drawing upon the ULCC's Act in drafting its own report on model electronic records legislation for small member states in the Commonwealth of Nations.[32] However, despite its general adoption in Canada and its influence abroad, the UEEA has received very little judicial consideration or application in the past twelve years.[33] Why is this the case?

In our view, as the years have gone by and the implications of the pervasive use of digital technology (including electronic mail) for the law of evidence have become better understood, the limitations of the Act have resulted in the courts' continuing reliance on traditional, narrow common law rules rather than broader, new statutory rules. These limitations are in part due to the fact that the UEEA focuses on authentication and the best evidence rule, with scant attention paid to the hearsay rule and the business records exceptions, the application of which requires a clear concept of record and a clear methodology for identifying records in digital systems. Additional and more important limitations include the absence of provisions related to the search and seizure of electronic records in both civil and criminal cases;[34] the protection of privacy; the ever-expanding retention and preservation duties for electronic records on the part of law enforcement offices, legal offices, and the courts; the spoliation, or purposeful destruction of electronic records to escape prosecution; and e-discovery. However, it is best to begin with an analysis of what the Act states and of the manner in which its statements are expressed.

Analysis of the *Uniform Electronic Evidence Act*

In the Act, the ULCC shifted the focus of the authentication and best evidence rules from the record to the electronic system in which the record is contained, inferring trustworthiness from the integrity of the system, rather

31 See also the *B.C. Evidence Act*, subsection 41.2(2).

32 Commonwealth Secretariat, LMM(02) 12, "Draft Model Law on Electronic Evidence," para. 4, available at http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BE9B3DEBD-1E36-4551-BE75-B941D6931D0F%7D_E-evidence.pdf (accessed on 20 May 2010).

33 For example, *Coco Paving (1990) Inc. v. Ontario (Transportation),* [2009] ONCA 503; *College of Opticians of British Columbia v. Coastal Contacts Inc.,* [2008] BCSC 617; *R. v. Blumes*, [2002] BCPC 45.

34 On the issue of search and seizure, see for example, *R. v. Bishop*, para. 20–47.

than ascertaining it from the form of the record and its status as an original.[35] If the litigant offering an electronic record as evidence can show that the system producing or storing it operates the way it is expected to, the output satisfies the evidentiary requirements, regardless of its form. The ULCC commentary following paragraph 1(b) of the Act states: "This Act focuses on replacing the search for originality, proving the reliability of systems instead of that of individual records, and using standards to show systems reliability." As a factor in determining the reliability of a system, section 6 of the Act replaced the traditional identification of individual records by a witness or other foundation evidence with proof of compliance of the system with recognized records management standards, procedures, usages, or practices.

The Act comprises nine sections, the first defining for the purposes of the Act the key terms used in it; the second establishing the limits of its application; the third providing for the application of the authentication rule; the fourth for the application of the best evidence rule; the fifth for the presumption of integrity; the sixth discussing the use of standards in support of the evidence offered; the seventh providing for a proof by affidavit; the eighth discussing the right of cross-examination; and the ninth advising that statutory rules requiring that the retention of paper originals of microfilmed records should be repealed. Each section includes paragraphs or subsections, which are the provisions or rules, each followed by comments having the purpose of explaining the rule or its application.

Section 1: Definitions

Like most statutes, the Act begins with definitions. In our view, its definitions are its major weakness because they are inconsistent with the current terminology in the electronic environment as it has developed in the context of research projects (e.g., the International Organization for Standardization's [ISO] and other national and international standards), and records management best practices.

Paragraph 1(a) states: **"data" means representations, in any form, of information or concepts**. According to the commentary, the intent of paragraph 1(a) is to include in the concept of data any form of information that can possibly be part of the content of an electronic record, whether facts, figures, or ideas. The Province of Alberta is the only jurisdiction not to use the definition of "data" in its enactment of the Act. Section 41.1 of the *Alberta Evidence Act* omits the definition of "data," and simply refers to

35 According to diplomatics, the degree of perfection of a record is measured by its status of transmission – that is, whether it is a draft, a copy, or an original. The degree of perfection is lowest in a draft and highest in an original, which can, however, be substituted by an authentic copy.

"information."

Paragraph 1(b) states: **"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred to in subsection 4(2)**.[36] This definition suggests that the defining characteristics of an electronic record are its method of inscription and capacity for access. Contrast this with the archival definition of a record: a document made or received by a physical or juridical person in the course of practical activity and kept for action or reference. In enacting paragraph 1(b), some jurisdictions, including the federal one, have replaced the phrase "electronic record" with "electronic document."[37] Indeed, by considering the fact of being a recording by a computer or similar device (which is the primary identifying characteristic of an electronic record), the Act provides an incomplete definition of record and ends up defining a document. Any information recorded by, or stored in, a computer or similar device, then, is considered an electronic record by the terms of the Act, and the qualities that would establish it as a record according to archival and diplomatic theory do not become relevant until tests for admissibility are applied.

In fact, paragraph 1(b) is insufficient to identify an electronic record in such a way that the business records exception to the hearsay rule and the best evidence rule can be easily used; is also unclear and imprecise in what it does state. The phrase "computer system or other similar device" and the related commentary are confusing as to the phrase's intended scope, in that a similar device can be external storage in a CD ROM, a magnetic tape, a backup drive, or a cellular telephone. The commentary says the definition does "not apply to telexes and faxes (except computer-generated faxes)," but these devices involve computer-like operations that generate and store information on the date and time of transmission, identification of intended sender and recipient, and success or failure of the transmission. Similarly, the commentary says the definition does not apply to "regular digital telephone conversations," which, although not recorded, leave recorded traces in the same manner as faxes and telexes; and what about mobile telephones, text-messaging, and other similar communications? According to the commentary, video is not covered

36 Subsection 4(2) states: "[In any legal proceeding] an electronic record in the form of a print-out that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, is the record for the purposes of the best evidence rule."

37 Canada, *Canada Evidence Act*, section 31.8; Manitoba, *Manitoba Evidence Act*, section 51.1; Northwest Territories and Nunavut, *Evidence Act*, subsection 37.1(1); and Ontario, *Evidence Act*, subsection 34.1(1).

by the Act, but computerized music and videos are included in the concept of data, thereby considering recorded music and videos "information," and requiring their compliance with the strictures of the statutory requirements of authentication and best evidence. Prior to the Act, music, and still and moving images did not have to comply with the traditional best evidence rule, because they did not entail proof of verbal/numerical contents or "information," though at common law they require authentication.

A further example of lack of precision in the commentary is the statement that the definition of electronic record applies to data that can be "read or perceived" by a computer or other similar device: if the data are only machine-readable, they are unintelligible to the judge and jury. Should they be inadmissible in a court of law?[38] Later on, the commentary seems to clarify this by stating that "paper records that are produced directly by a computer system, such as printouts, are themselves electronic records, being just the means of intelligible display of the contents of the record"; however, a photocopy of a printout from a computer is a paper record and subject to the "usual rules about copies," which means the common law best evidence rule would apply. The commentary says that when a printout is used as the record of an action, the electronic version ceases to be "the record" for the purposes of the "best evidence rule," referring to subsection 4(2). The last phrase in paragraph 1(b), which lists types of electronic records, mentions displays, printouts, and other computer outputs, but expressly excludes from the category of electronic records those "referred to in subsection 4(2)," that is, those printouts that acquire a record function in place of their electronic version. This presents a problem when a party keeps both a printout and an electronic version of the same item and uses them interchangeably. When a discrepancy develops between the two versions, subsection 4(2) says the paper copy is "the record," which means it would prevail over the electronic version, because it would qualify as having been consistently relied on, even though the same could be said of the electronic version. The commentary does not discuss the status of the digital copies of scanned records.

Paragraph 1(c) states: **an "electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records**. The definition includes within a system not only operating equipment and a variety of storage media ("the computer system or other similar device") but also the rules that control the creation, storage, access, security, verification, retention, and destruction of electronic records, regardless of whether they were followed. Despite the exclusion of records

38 *Powell v. Lenthall*, [1930] HCA 43, 44 C.L.R. 470; *R. v. Minaoui*, [2004] VSCA 126; but see *R. v. Bell and Bruce* (1982), 26 C.R. (3d) 336, affirmed without reasons, [1985] 2 S.C.R. 287.

from the definition of records system, in the commentary the paragraph addresses "procedures" in relation to such matters as "physical and electronic access controls," and "retention or destruction schedules," that is, in relation to records management. However, further on, section 4 contradicts this early emphasis on records management by saying that "records retention policies, for paper or electronic records, are beyond its [the Act's] scope, and should not be determined by the law of evidence in any event." This assertion defies the statutory and common law rules relating to proof of authenticity by "chain of custody," duties of preservation of evidence, destruction or spoliation of evidence and their evidentiary consequences (such as drawing adverse inferences), etc. In addition, the assertion conflicts with section 6 of the Act, which requires a presiding judge to take into account a "standard, procedure, usage, or practice" when applying any rule of law governing admissibility of records, thereby making records management pivotal in a judge's decision as to admissibility, a decision that becomes part of the law of evidence.

Thus the definitions of data, electronic record, and electronic records system lack usefulness to the applicability of the admissibility rules of authenticity, best evidence, and hearsay to electronic records. Moreover, they are not sufficient to clarify the meaning of all provisions. Some jurisdictions have added definitions of additional terms to their enactment of the Act. For example, Canada and Manitoba added a definition of "computer system" to their legislation,[39] although such definition suffers from circularity. It states that a "computer system" is "a device that, or a group of interconnected or related devices one or more of which, a) contains computer programs or other data, and b) pursuant to computer programs, performs logic and control, and may perform any other function."

In our view, other terms used in the Act should also be defined. For example, subsection 4(1) of the Act speaks of the "integrity of the electronic records system," but "integrity" is not defined in section 1, and the commentary to the Act refers to integrity as the equivalent of "reliability." Alberta implicitly included incorruptibility and completeness as essential qualities of integrity by enacting its unique subsection 41.1(2), which emphasizes the relevance to integrity of "reliable encryption techniques."[40] This subsection, which is only contained in the *Alberta Evidence Act,* states: "The integrity of an electronic record may be proved by evidence of the integrity of the electronic records system by or in which the information was recorded or stored, or by evidence that reliable encryption techniques were used to support the integrity of the electronic record." However, a

39 Canada, *Canada Evidence Act,* section 31.8; Manitoba, *The Manitoba Evidence Act*, section 51.1.

40 Alberta, *Alberta Evidence Act*, 41.1(2).

clear definition of integrity is essential to the applicability of both the authentication and the best evidence rule, the determination of which should be based on a strong foundation of evidence consistent with clear conceptual, not technological parameters.

Similarly, as mentioned above, section 6 of the Act refers parties and the courts to "a standard, procedure, usage, or practice" as important to admissibility, but the Act does not define or rank these terms. Is an internationally recognized or a governmental "standard" intended to have more authority in determining admissibility than a localized or specialized "usage" or "practice?" In the absence of statutory definitions for these terms, their meaning is uncertain until courts interpret them. Unfortunately, given the minimal judicial consideration of the Act to date, the courts have not helped in the interpretation of this section. Thus, it would be useful not only to define in the Act what a standard is but also to indicate what standard or family of standards should be adopted, because, like legislation, standards contain definitions which could ensure consistency in the interpretation of the Act for both those who need to offer electronic records as evidence and those who need to determine their admissibility.

It would have been useful if the Act had clearly addressed the hearsay aspects of computer records. The common law distinguishes between records produced by systems without human intervention (such as mechanical calculations beyond manual computation, or where the device gathers information on its own initiative by monitoring and recording conversations) from records compiled by humans within electronic systems. At common law, records generated by computers without human intervention are non-hearsay, and are admissible as real evidence rather than as statements made by persons.[41] As real evidence, the Act provides guidance on authentication by a witness qualified to explain how the device operates, which is all that is required for admissibility.[42] Records produced with human intervention are classified as hearsay at common law, but are admissible nevertheless if they fit within an exception to the hearsay rule, are authenticated, and constitute the best evidence. The Act provides guidance only on the second-tier issues of authentication and best evidence but does not deal with the primary question of admissibility, which is the hearsay rule.[43] One must go outside the Act to find an existing common law or statutory exception, or the principled approach. The Act itself does not create a new exception to the hearsay rule, which is a serious omission in our view, and leaves a critical question unanswered within its own provisions.

41 *R. v. Hall*, [1998] CanLII 3955, [1998] B.C.J. No. 2515(OL) (S.C.).
42 *D.P.P. v. Colm Murphy*, [2005] IE CCA 1 (Irish Court of Criminal Appeal).
43 *R. v. L.B.*, [2009] B.C.J. No. 1741 (OL) (S.C.).

Finally, considering the centrality given to the integrity of the system containing the record to determine the record's authenticity, it would be useful to add a definition of record-keeping system to the Act. Both the Canadian standard *Electronic Records as Documentary Evidence* (CAN/ CGSB-72.34-2005) and the record-keeping family of ISO standards serve as a reference for such a definition.

Section 2: Application of the Act

This section of the Act explains the relationship between the subsequent provisions and existing evidentiary rules, but does so in an internally contradictory way.

Subsection 2(1) of the Act and the related commentary state that the Act modifies only the evidentiary rules about best evidence and authentication. Contrary to this assertion, however, the commentary to section 3 on authentication says that the Act "codifies" the common law, which in this context means that it declares the existing common law without modification. If this is true, there cannot be enactment of subsection 2(1). This also contradicts subsection 2(2), which states that a court may have regard to evidence adduced under this Act in applying "any common law or statutory rule" to determine the admissibility of records, thereby extending the scope and application of the Act to exclusionary rules of evidence beyond best evidence and authentication, such as the hearsay rule and its exceptions.

Furthermore, admissibility of evidence is a matter for the presiding judge to decide. As mentioned above, in making a decision on whether or not to admit an item of evidence, the judge may have to examine foundation evidence relating to the issue of admissibility. The common law and statutory provisions prescribe the considerations for the judge in determining admissibility. Sections 4 and 6 of the Act add other factors for the judge to consider to those prescribed considerations when determining the admissibility of electronic records. Subsection 4(1) of the Act makes evidence of the "integrity of the electronic records system," a consideration for the judge who is deciding on the admissibility of electronic records under the best evidence rule. However, subsection 2(2) had already made the same evidence admissible. Section 6 purports to affect the admissibility of electronic records under "any rule of law" by authorizing the admissibility of a "standard, procedure, usage, or practice" relating to recordkeeping as foundation evidence, but, subsection 2(2) had also already covered the scope of section 6. Some phrase linking the provisions would be helpful to clarify whether subsection 2(2) or section 6 prevails in the event of a conflict with subsection 2(1).

Section 3: Authentication

The purpose of this section of the Act is to codify the common law rule of authentication, requiring a person offering an electronic record as evidence to lay a foundation for its admissibility, by presenting to the presiding judge evidence that the record is what the person claims it to be.[44] In this context, the reference to a "person" is ambiguous as the term could refer to a litigant or a witness, such as the witness who will authenticate the record. To differentiate between the roles of litigants and witnesses in regard to authentication, some jurisdictions replaced the phrase "what the person claims it to be" with the phrase "that which it is purported to be."[45]

The issue of whether this section merely codifies or actually modifies the common law has already been discussed. The commentary says: "The proponent needs only to bring evidence that the record is what the proponent claims it is (e.g., "This record is an invoice")." In our view, two omissions from a comprehensive definition of "authentication" are apparent in this passage: (1) the proponent must prove authenticity on a balance of probabilities (not merely introduce evidence capable of supporting a finding);[46] and (2) the proponent must not only prove that "This is an invoice," but also relate it to the issues in dispute in the litigation as part of authentication, by stating whose invoice it is and what is its significance.[47] This concept of authentication as legislated is legally incomplete, rather than fully articulated. In fact, the commentary states: "The Act does not open an electronic record to attacks on its integrity or reliability at this stage. That question is reserved for the new 'best evidence' rule. Logically the question of integrity could be included in authentication, but the Conference decided that the question should be dealt with only once." The grounds for such a decision are not explained, although they are implicitly stated in the following section; one can see, however, that by separating identity and integrity it would be possible to authenticate an electronic record of questionable integrity. Although traditionally the law has linked authentication to the ascertainment of the identity of a record, and the best evidence rule to an inference of integrity made from the degree of perfection of the record (i.e., the original is the first, complete, effective record), with electronic records, given the absence of an original, the two qualities of identity and integrity are interwoven to the point of being interdependent.

44 *Ross v. Redl Estate*, [2008] SKQB 298, [2009] 3 W.W.R. 166, para. 26 and 27.

45 The jurisdictions are: Canada, *The Canada Evidence Act*, section 31.1; Manitoba, *The Manitoba Evidence Act*, section 51.2; Northwest Territories and Nunavut, *Evidence Act*, subsection 37.1(4); Ontario, *Evidence Act*, subsection 34.1(4).

46 *R. v. Evans*, [1993] 3 S.C.R. 653, [1993] S.C.J. No. 115 (QL).

47 *Lowe v. Jenkinson,* [1995] B.C.J. No. 216 (QL); 5 B.C.L.R. (3d) 195 (S.C.).

Section 4: Application of the Best Evidence Rule

The exclusion of integrity from consideration in the application of the authentication rule becomes clear when reading this section on the application of the best evidence rule. The best evidence rule at common law applies where a party seeks to prove the contents of a document, and purports that the best or primary evidence is the original document. Secondary evidence, such a copy of the document, a witness's recollection of what the document said, or a handwritten summary of the contents, is inherently suspect and the original is preferred if it is available. Where evidence of the contents of an electronic record is offered, subsection 4(1) states that the integrity of the electronic record-keeping system is a substitute for the traditional common law preference for the original. Subsection 4(1) only modifies, rather than abolishes, the necessity to offer the best evidence if a party wishes to prove the contents of an electronic record. Failure to satisfy the judge that the electronic record is the best evidence will result in its exclusion from the evidence in the case.[48] However, this section greatly reduces the requirements for best evidence by focusing only on the integrity of the system. As Heather MacNeil writes,

> … the epistemically best evidence is … that which is most complete. The dimension of completeness is particularly pertinent to electronic records since structural and contextual elements of an electronic record may be stored separately from its content. In an electronic recordkeeping environment, adherence to a best evidence principle would entail an obligation on the part of the litigating parties to produce the record that contains all the relevant structural, contextual, and discoursive elements … The foundation evidence supporting a presumption of integrity should be capable of demonstrating not only the reliability of data input and verification procedures, but also the completeness of the procedures for reproducing original presentation features and annotations, to the extent that these are relevant to an understanding of the record's content … This would entail, in turn, an obligation on the part of courts to come to grips with the question of what precisely constitutes a complete record and to assess the significance of missing elements.[49]

This section, by underestimating the complexity of electronic records and of the systems producing and containing them, weakens the application of the best evidence rule practically to irrelevancy. Moreover, it conflicts with the corresponding sections of other general evidence acts, that permit secondary evidence provided by government, court, and business records to be introduced in support of the reliability of the content of the records offered in evidence.

48 *R. v. Bellingham*, [2002] A.J. No. 476 (QL), 2002 ABPC 41.
49 Heather MacNeil, *Trusting Records*, p. 56.

Subsection 4(2) of the Act codifies a common law rule that came about in relation to a bank branch printout of account activities as "the record" for purposes of satisfying the traditional best evidence rule.[50] Subsection 4(2) states that, if a printout is relied or acted on as the authoritative "record" of activities, it becomes the best evidence in the traditional sense of proof of the transactions recorded there. A printout that qualifies as "the record" under subsection 4(2) becomes the best evidence in the traditional common law sense, and not under the new best evidence rule formulated in subsection 4(1), as a result of the phrase, "other than a printout referred to in subsection 4(2)." To clarify that subsection 4(2) contradicts subsection 4(1), some jurisdictions added the phrase "despite subsection (1)" to their enactments of subsection 4(2).[51]

Subsection 4(2) essentially allows the out-of-court practices of the party that makes and keeps the records to determine the question of when a printout is acted upon with sufficient consistency to qualify as "the record," with the exclusion from admissibility of other forms of the same record, even if they have not been destroyed and are still used. On the other hand, in the event of a disparity between the electronic version and that contained in a printout, if the business relies on the electronic version of the same record as more accurate, presumably the printout would be inadmissible under subsection 4(2), and the opponent could not introduce it as evidence in support of its version of the transaction. In other words, the person offering the record in evidence makes the choice of what version of a record existing in more than one version is the most accurate based on frequency of use; following this, both parties have to accept the record identified as the best evidence as such. This is consistent with what is stated in the commentary to the previous subsection, according to which, if an image is produced by scanning original paper records, it is up to the party offering the record as evidence to decide whether to submit the scanned image as best evidence (which would be assessed on the basis of the integrity of the system containing it), or the paper original (which would be assessed on the basis of the best evidence rule at common law).

While it is a high point of principle that the record of a person or organization is that which is used in the usual and ordinary course of business for the purposes of the business (and later for reference), this presumes the admissibility of only one version of each record, either the born-electronic record or its printout, or either the paper record or its image. This blanket rule of allowing the decision on whether to submit a printout or its electronic counterpart, an electronic image or a paper original, if both exist and are used

50 *R. v. Bell and Bruce*.

51 These jurisdictions are: Canada, *Canada Evidence Act*, subsection 31.2(2); Manitoba, *Manitoba Evidence Act*, subsection 53.2(2); Ontario, *Evidence Act*, subsection 34.1(6); and Northwest Territories and Nunavut, *Evidence Act*, subsection 37.1(6).

by the party offering the evidence, seems to turn the best evidence rule away from its traditional purpose of protecting the courts from unreliable evidence. These provisions are open to abuse by a recordkeeper who, for example, astutely follows a practice of relying on self-serving printouts as authoritative.

Section 5: Presumption of Integrity

This section of the Act creates legal presumptions in favour of the integrity of an electronic records system. Legal presumptions create rules of law that, in this context, enable a litigant offering an electronic record into evidence to satisfy the judge that the electronic records system containing it possessed the "integrity" required by subsection 4(1) by proof of other facts, as defined by the paragraphs. If the party can establish those other facts, the judge must make a finding that the system satisfies subsection 4(1), without requiring the party to prove "integrity" directly rather than by inference from the established facts. The purpose of these presumptions is to facilitate the admissibility of electronic records by offering alternative ways of proving their integrity through establishing the "integrity of the electronic records system."

The presumptions of integrity are rebuttable by the opposing party. They require an opposing litigant who wishes to dispute admissibility of an electronic record to make an objection of substance by offering "evidence to the contrary," and not to make a serious issue out of an insubstantial or technical objection that the electronic record is not the best evidence. In a criminal case, the defence need only raise a reasonable doubt to rebut the presumption; and if the defence is successful in rebutting the presumption, the Crown can prove the integrity of the electronic records system by reliance upon another presumption or by introducing admissible evidence of integrity.[52] To satisfy the requirement of "evidence to the contrary" in a civil case, an opposing litigant must meet a higher standard of proof than an accused in a criminal case: the civil opponent must meet the standard of proof on a balance of probabilities to rebut the presumption.[53]

Paragraph 5(a) creates legal presumptions to the effect that the judge must accept the claim of integrity for an electronic records system if credible evidence is offered that the system operated properly at all material times, or any improper operation did not affect the "integrity of the electronic record" and, apart from the improper operation that had no effect on the record, the integrity of the system was not assailed. In many cases it might be reasonable and fair to presume the reliability of a computer system, but the computer

52 *R. v. St. Pierre*, [1995] 1 S.C.R. 791, 112 D.L.R. (4th) 619.
53 *Pecore v. Pecore*, [2007] 1 S.C.R. 795, 2007 S.C.C. 17, at para. 24–26.

system to which the Act refers is one that is used for recordkeeping, and such a system involves interactions with human beings. The human element might raise doubts about human error or falsification, particularly for data contained in records made, received, or stored after a dispute has arisen. Also, when long-term preservation and accessibility of electronic records are involved, as is more frequently the case, systems can break down or become obsolete. One wonders whether the presumption of integrity of a computer system should apply regardless of the length of time elapsed from when a record was created or used to when it is offered as evidence. This is especially worrisome in the context of section 5(b) discussed below, which puts the onus of proof on the party who does not know the system and the procedures; in contrast, the law of evidence usually puts the onus on the party with the better means of knowledge.

Current expectations and legal requirements about how long certain electronic records must be preserved are increasing, thereby necessitating the permanent preservation of some records with high potential for use as evidence. This raises concerns about the practicality of requiring evidence of proper operation of the system "at all material times." For example, consider the following recommendation from the Milgaard Inquiry: "All prosecution and police files, including police notebooks, relating to indictable offences should be retained in their original form for a year, then scanned and entered into a database where a permanent, secure electronic record can be kept."[54]

In legal proceedings in which pre-trial discovery or disclosure of documents occurs, paragraph 5(b) applies the presumption of integrity of the system to electronic records recorded or stored, and produced by an adverse party. The party which obtained the production of the records has the benefit of this presumption to facilitate the admissibility of the opponent's electronic records, but not the adverse party who was obliged to produce the records, which supposedly has a better knowledge of the system.

The concept of parties who are "adverse" or "adverse in interest" applies more aptly to civil than to criminal proceedings, because the Crown and the accused are not necessarily in the same adversarial relationship as opposing civil litigants. In a criminal proceeding, the Crown must make disclosure of all its potentially relevant evidence to the defence, but not vice versa. There is no obligation on the defence in a criminal case to make equivalent disclosure of its evidence. It has been held that the Crown owes a duty to disclose evidence that might benefit the defence even though it is not, strictly speaking, "adverse in interest" to an accused in disclosing it.[55] One cannot

54 The Honourable Mr. Justice Edward P. MacCallum, *Final Report of the Commission of Inquiry into the Wrongful Conviction of David Milgaard* (2008), available at http://www.milgaardinquiry.ca (accessed on 8 June 2010).

55 *R. v. MacNeil*, [2009] SCC 3, 238 C.C.C. (3d) 353, at para. 13 and 50.

help wondering whether, if the defence decides to introduce the evidence disclosed by the Crown, it can rely on the presumption in paragraph 5(b) to support the admissibility of the evidence, since an adverse party did not make the disclosure. Clearly, this question arose in the context of the *Canada Evidence Act*, subsection 31.3(2), where the adjectival phrase, "adverse in interest" is replaced by the adjective "adverse," thereby opening the issue to interpretation.

Paragraph 5(c) reflects the traditional concerns of an adversarial system of trial that suspects a record generated by, or on behalf of, a party to litigation, especially if this has happened any time after the dispute has arisen or was expected. The adversary system would be ill-served by offering temptation to litigants to generate and introduce self-serving evidence once litigation is underway or reasonably anticipated. In furtherance of that spirit, paragraph 5(c) presumes integrity if the person who created or stored the electronic record is not a litigant in the proceedings or under the control of a litigant, and if the person created or stored the record as a regular part of a routine or system. The phrase in paragraph 5(c), "usual and ordinary course of business," has become synonymous with "routinely," "systematically," or "regularly."[56]

The problem is that paragraph 5(c) makes the assumption that the parties to litigation are always joined as they should have been; sometimes, however, litigation is not set up properly and all the appropriate parties are not joined in the proceeding. Also, the person who created or stored the electronic record might have had an interest in the outcome of the litigation, even though not a party to it or under the control of a party. The opponent would have to raise these matters as "evidence to the contrary," in an attempt to rebut the presumption.

Section 6: Standards

Section 6 states that the judge may consider evidence of a "standard, procedure, usage, or practice" in determining admissibility of electronic records under "any rule of law." This extends the Act beyond best evidence or authentication purposes to any rule of law governing admissibility, such as the hearsay, character, or opinion rule. This section thus contradicts section 2(1), which purports to limit the scope of the Act to the two rules: best evidence and authentication.

We are concerned that the section and the commentary might be interpreted as taking authority away from presiding judges over questions of

56 *Young v. RBC Dominion Securities*, [2008] CanLII 70045, [2008] O.J. No. 5418 (QL), 2008 CarswellOnt 8158 (S.C.), para. 165.

admissibility of electronic evidence in legal proceedings, and vesting authority to determine them in records professionals, or by agreement of the parties, through application of "standards, procedures, usage, or practice." A records professional or a litigant might misread this provision and the commentary as offering an assurance ("take comfort") of guaranteed admissibility for records kept in accordance with "a standard, procedure, usage, or practice" of the records professional's own choosing, or with the litigant's agreement.

We believe that this interpretation is incorrect in the broader context of common law, and that records professionals should not presume that following standards or best practices will ensure that the records they are responsible for will be admissible in a court of law. Judges decide factual issues around admissibility of disputed evidence, including electronic evidence, not the parties or records professionals. For example, judges do not regard themselves as necessarily bound by parties' records retention schedules. In criminal cases, judges often reject retention periods adopted by the police for its own records if they are unreasonably brief and the evidence might have assisted the defence. Sometimes, the judge orders a stay of proceedings because destruction of the evidence violated the accused's *Charter* rights.[57]

The phrase "standard, procedure, usage, or practice" covers a wide range of possibly contradictory, and, as the commentary to this section acknowledges, constantly evolving guidelines. The commentary identifies two "gold" standards of admissibility, specifying those issued by the Canadian General Standards Board (CGSB) and by ISO. The CGSB is an agency of the federal government that develops voluntary standards in various fields using the expertise of standards committees. The current versions of these standards are: *Electronic Records as Documentary Evidence Standard*, CAN-CGSB 72.34 (2005); *Microfilm and Electronic Images as Documentary Evidence Standard*, CAN-CGSB-72.11-93; and *Electronic Imaging–Information Stored Electronically–Recommendations for Trustworthiness and Reliability*, ISO 15801:2004. However, as mentioned above, the definitions contained in these standards are inconsistent with those of the Act and the guidelines provided by these standards are more often than not in conflict with the provisions of the Act.

The commentary to section 6 states that a specific litigant's own unique records management program can qualify as a "standard," but we believe it should more accurately be referred to as a formally accepted and implemented policy, containing procedure and practices. The commentary suggests a party's own "standard" would carry at least equal authority with other standards, etc.,

57 *R. v. Maghdoori*, [2008] ONCJ 129, 166 C.R.R. (2d) 157; *R. v. Leung*, 2008 ONCJ 110, 171 C.R.R. (2d) 300; but see *R. v. Badgerow*, [2008] 58 C.R. (6th) 367, 169 C.R.R. (2d) 348 (Ont. C.J.).

but such matters are for the judge to decide in the circumstances of each case and it would not be advisable for records managers to count on this suggestion. Assessing a party's conduct according to the standard of a "well accepted practice" has been held to be inappropriate in another context;[58] even though the commentary approves of it, judging a party's conduct by compliance with the party's own "practice," could lead to pointless circularity.

On the issue of admissibility, section 6 allows records professionals to present evidence for and against the merits of various policies, including those that were followed and ignored. In determining admissibility, it would be up to the judge to decide which policy was appropriate in the circumstances and whether the creation, maintenance, and preservation of the disputed electronic record complied with the policy.

Once the electronic evidence is ruled admissible, the trier of fact (judge or jury) can receive and consider it in its deliberations. Curiously, section 6 does not refer to weighing the evidence, only to determining admissibility. The role, if any, of a standard, etc., in determining the weight of evidence is left open.

Section 7: Proof by Affidavit

Section 7 states that, instead of having to call witnesses to prove by their testimony the matters under subsection 4(2), and sections 5 and 6, these matters can be proven by affidavit. The witnesses do not need to attend the court proceeding to testify, unless the other party wants to cross-examine them under section 8 of the Act. There are many similar provisions in statutes and rules of court. The affidavit can contain hearsay ("based on information and belief") and does not require the source to be identified, in contrast with other provisions at common law that permit hearsay in affidavits but require the disclosure of the name of the source of the hearsay. It is questionable how the cross-examiner could get anywhere with the cross-examination of a deponent on an affidavit when the deponent lacks personal knowledge of the facts deposed to, and does not reveal the identity of the source of the hearsay contained in the affidavit.

Section 8: Cross-examination

Section 8 establishes the right of cross-examination by the adverse party, but this might not be as fair to the opponent as it might appear if the person who swore the affidavit (the deponent) has no personal knowledge and the affidavit is full of rumour. There is no provision to order costs against a civil litigant who unreasonably requires the attendance of a deponent for cross-

58 *The Royal Trust Co. v. M.N.R.*, [1957] C.T.C 32, 57 D.T.C. 1055 (Exch. Ct.).

examination, as is quite common in other contexts where the object of the provision is to shorten the length of trials by dispensing with the unnecessary attendance of witnesses.

Section 9: Repeal

Section 9 establishes that, except for Computer Output Microfilm, microfilmed records are not strictly "electronic records" within the scope of the Act. Nevertheless, the Act goes out of its way to recommend repeal of an exclusionary provision existing in some evidence acts. The general evidence acts of Canadian jurisdictions provide for the admissibility of microfilmed copies of paper documents. Some of these provisions confer upon the presiding judge discretion to exclude a microfilmed copy if the paper document was destroyed or lost within six years. The period of six years runs from the date at which the paper document would have been destroyed in the ordinary course of business (meaning routinely), or the date of notice of a claim to which the document relates. Exemptions variously protect admissibility of microfilmed government, court, or Bank of Canada records from the exclusionary discretion.

The ULCC, in the commentary to section 9, argued that microfilmed records should be admissible, given sufficient support of their integrity, regardless of the time of destruction or loss of the paper version. The Conference recommended repeal of the exclusionary discretion, so that the parties' wishes would prevail over the power of the courts to exclude microfilmed documents in favour of their paper originals. The recommendation did not affect the many Canadian jurisdictions whose evidence acts did not provide for an exclusionary discretion relating to microfilm. Only three of the concerned jurisdictions accepted the Conference's recommendation.[59] The remainder rejected the recommendation and retained their exclusionary discretions.[60]

Conclusion

The fundamental concerns of the law of evidence with any type of evidence, including electronic records, are relevance, admissibility, and weight. To

59 Nova Scotia, *Evidence Act*, section 22 [2002, c. 17, section 1]; Ontario, *Ontario Evidence Act*, section 34 [1999, c. 12, Sch. B, subsection 7(1)]; Yukon Territory, *Yukon Evidence Act,* section 40 [2000, c. 11, section 9].

60 Alberta, *Alberta Evidence Act*, subsection 40(3); Manitoba, *The Manitoba Evidence Act*, subsection 51(3); New Brunswick, *Evidence Act*, subsection 47(3); Newfoundland and Labrador, *Evidence Act*, subsection 27(3); Northwest Territories, *Evidence Act*, subsection 48(3); Prince Edward Island, *Evidence Act*, subsection 31(3).

lawyers, judges, and others looking for guidance on the application of these concepts to computer-generated or stored evidence, the UEEA offers rules of admissibility focusing on authentication and best evidence tied closely to the computer technology of the 1990s. The Act does not provide any guidance with respect to issues of relevance or weight, and offers only cursory reference to other rules of law such as the hearsay rule.

In its current form, the Act is subject to the criticisms that it perpetuates the increasingly irrelevant best evidence rule, fails to address hearsay issues, and conflicts with existing statutory exceptions.[61] The most important failing of the Act, however, is its misleading treatment of electronic evidence as susceptible to governance by one set of brief rules that presupposes a fixed technology. While this approach might have been appropriate back in 1997–1998 when the Act was developed, the subsequent growth of digital technology has made it untenable. Digital technology raises the most profound challenges yet to the traditional evidentiary concepts of relevance, admissibility and weight, and puts into question the very idea of record as embedded in the admissibility rules of the law of evidence. In addition, the common understanding of relevance and weight is more open than ever to scrutiny in the digital world. When the Act was formulated, the profound impact of digital technology was not fully comprehended, and the Act suffers as a result.

The implications of digital technology for the law of evidence are becoming better understood thanks to the contribution of various disciplines, among which diplomatics and digital forensics are prominent. While diplomatics has developed a detailed theory of what is a record in the digital world, digital forensics has delved into the complexity of digital systems and articulated the requirements for assessing their integrity. Both disciplines are having a strong impact on the meaning of best evidence and, in relation to it, of authenticity, and on the assessment of what qualifies as hearsay.

As it regards best evidence, diplomatics has demonstrated how the concept of originality – which has lost its traditional meaning in the digital environment – can be substituted by the concepts of record identity and integrity, as determined and revealed by the metadata linked to the record. As it regards hearsay, digital forensics has brought to the fore the distinction between "computer-generated records," or statements produced by computers without human intervention, and "computer-stored records," or statements produced by humans using computers, and suggested that only the latter can be considered hearsay and be admissible under the business records exception to the hearsay rule. On the other hand, computer-generated records can only be admissible on the basis of their authenticity as inferred from the integrity

61 See Chasse.

of the system in which they reside.[62]

Digital evidence includes not only business records introduced by a litigant or defence counsel, but also materials that may be found in seized computer hard drives and backup media, real-time email messages, chat-room logs, ISP records, web pages, digital network traffic, local and virtual databases, digital directories, wireless devices, memory cards, and digital cameras.[63] These belong not only to business enterprises, but to private individuals. How can the context of the extracted information be presented and understood, and subsequently protected, in such a way that the integrity of the data is preserved? What are the rules of admissibility for such evidence?

We believe that these and other positions taken by diplomatics and digital forensics, together with the new understanding of digital records fostered by recent archival and legal research, suggest that dramatic changes to the Act are required, and that a new field of interdisciplinary knowledge needs to emerge that will provide the conceptual and methodological foundation for these changes. Successful legislation aimed at regulating the admission into evidence and the decision about relevance and weight of electronic records must result from an integration of the knowledge and perspectives of the legal and law enforcement professions, the records professions, and the information technology profession. Such an interdisciplinary approach will not only relieve inconsistencies in interpretation of electronic evidence, but also help individuals and organizations understand how they can create, maintain, and preserve digital materials to best ensure admissibility if they find themselves involved in legal action. But integration is difficult as all these professions have established systems of beliefs, theories, and methodologies; a dedicated, collaborative research effort is therefore required to reconcile conflicting ideas and to overcome inconsistencies by developing new concepts, principles, and methods that both incorporate and transcend established ideas.

In this spirit, the present authors are conducting a research project[64] that,

62 George L. Paul, in *Foundations of Digital Evidence* (Chicago, 2008), pp. 141–45, argues persuasively that many computer-generated records are declarative statements that are indeed hearsay despite being twice removed from the courtroom. Thus, he believes that a second exception to the hearsay rule is warranted, which considers admissible computer-generated records that were created and reside in a system whose integrity can be proven. This would be the "system reliability" exception to the hearsay rule. Note the similarity to the Act rule that substitutes the system integrity requirement for the best evidence requirement. But see Nathan Wiebe, "Regarding Digital Images: Determining Courtroom Admissibility Standards," *Manitoba Law Journal*, vol. 28, no. 1 (2000), p. 61.

63 Chet Hosmer, "Proving the Integrity of Digital Evidence with Time," *International Journal of Digital Evidence*, vol. 1, no. 1 (2002), available at http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=article&id=9C4EBC25-B4A3-6584-C38C511467A6B862 (accessed on 22 May 2010).

64 The Digital Records Forensics Project is a collaboration among the University of British Columbia's School of Library, Archival and Information Studies (SLAIS), the Faculty of

starting from legal, diplomatic, forensic, and archival knowledge, aims at developing concepts and methods for identifying, authenticating, and acquiring digital records of individuals and organizations. These will allow the records management, archival, legal, judicial, law enforcement, and information technology professions to recognize records among all kinds of digital objects produced by digital technologies once they have been removed from their original system or changed from their original format, and to determine their authenticity. Methods and concepts are also being developed for maintaining records acquired from crime scenes or created by police to pursue crime over the long term so that their authenticity will not be questioned, and for addressing issues of privacy, privilege, and intellectual rights. This research is intended to form the theoretical and methodological content of a new discipline called "Digital Records Forensics," resulting from an integration of archival diplomatics, computer forensics, and the law of evidence with the project's newly developed knowledge.

It is hoped that it will not be necessary to wait for the end of this and other research projects before appropriate changes can be introduced in the law of evidence at both federal and provincial/territorial levels; it certainly would be useful to the legislator, however, to go beyond the legal field to gain an accurate understanding of the digital records environment and to find answers to the complex issues concerning definitions, relevance, weight, and hearsay that the Act has not answered or adequately addressed.

For electronic records to remain and be proved inviolate, for ensuring that "no sin … be committed against the … sanctity of archives through the wrongs done by wicked men," for not being all "compelled to grope in the dark, to feel our way with our hands"[65] but to be able to rely on our electronic records as evidence of our actions and transactions, present and past, it is essential that records professionals, participating in active citizenship, take part in the forging of legislative provisions that affect the use, management, and preservation of records and archives.[66]

Law of the University of Washington's School of Information, and the Computer Forensics Division of the Vancouver Police Department. The Social Sciences and Humanities Research Council of Canada generously supports the project. See www.digitalrecordsforensics.org (accessed on 20 May 2010).

65 Born, pp. 233, 237.

66 For example, the Sedona Conference, in issuing its principles for e-discovery, has made an effort to gain an understanding of records based on archival theory. Canadian records managers and archivists should seek the collaboration of the Sedona Conference. See the *The Sedona Canada Principles Addressing Electronic Discovery* (January 2008), available at http://www.thesedonaconference.org/dltForm?did=canada_pincpls_FINAL_108.pdf (accessed on 18 October 2009).

Appendix 1: The *Uniform Electronic Evidence Act*

1. In this Act,
   (a) "data" means representations, in any form, of information or concepts.
   (b) "electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred to in Sub-section 4(2).
   (c) "electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.

Application

2. (1) This Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.
2. (2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

Authentication

3. The person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Application of the best evidence rule

4. (1) [In any legal proceeding,] Subject to Subsection (2), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.
4. (2) [In any legal proceeding,] An electronic record in the form of a print-out that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, is the record for the purposes of the best evidence rule.

Presumption of integrity

5. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]
   (a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;

(b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Standards

6. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented [in any legal proceeding] in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, having regard to the type of business or endeavour that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

Proof by affidavit

7. The matters referred to in subsection 4(2) and sections 5 and 6 may be established by an affidavit given to the best of the deponent's knowledge or belief.

Cross-examination

8. (1) A deponent of an affidavit referred to in Section 7 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

8. (2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in paragraph 5(c).

Repeal

9. [Repeal provisions which require retention of original after microfilming.]