Regarding Digital Images: Determining Courtroom Admissibility Standards

NATHAN WIEBE*

I. INTRODUCTION

RAPID TECHNOLOGICAL ADVANCES IN recent years have brought fresh challenges to the law of evidence, which must be overcome. In the past, the law's response to the introduction of novel forms of evidence has been the development of doctrines which ensure admissibility, while satisfying concerns which courts have about the reliability and prejudicial effects of the evidence sought to be admitted. For example, evidentiary rules which are very form-specific are now applied to photographs and videotapes,[1] and rules based upon paper documents have been adapted to allow the admission of computer records.[2] Particularly, as scholars predict increased courtroom use of all types of real evidence, it is important to the facilitation of truth finding for the law to continue to keep pace with technological progress in this area.[3]

The proliferation of computers and their widespread usage in information systems has meant that many records and documents are being stored as digital images because of the convenience and cost-effectiveness of this storage method. This is a relatively recent technological innovation, and there exists some uncertainty about the standards of admissibility to be applied to digital

---

* Nathan Wiebe is proud to have been born and raised in the Province of Alberta. Having reached the age of majority in that province, he obtained a Bachelor of Arts degree at Wilfrid Laurier University in Waterloo, Ontario. He graduated from the Faculty of Law at the University of Victoria in May of 2000, and he is currently an associate at the firm of Gillespie Renkema Barnett Broadway in Kamloops, BC, doing primarily criminal prosecution work.

1 A.W. Bryant, S.N. Lederman & J. Sopinka, *The Law of Evidence in Canada*, 2nd ed. (Toronto: Butterworths, 1999) at 18–20.

2 *Ibid.* at 233.

3 *Ibid.* at 18; see generally the discussion in R. v. *Nikolovski*, [1996] 3 S.C.R. 1197.

images, given the unique characteristics of this new medium. Digital images have qualities which are comparable to both conventional photographs and to other types of computer-generated documents, but they also have peculiarities which are not addressed by evidentiary rules applicable to these other forms of visual evidence. It is desirable that policies or rules be developed which are clear, consistent and contemporary, so that parties dealing with digital images are able to know both whether particular records will be admissible as evidence in court, and what standards must be met in order to ensure record admissibility.

This paper begins with a brief overview of the nature and characteristics of digital images, accompanied by a discussion of why this technology challenges the application of traditional admissibility rules for documents. It then looks at the general rules of admissibility which are applied to both conventional photographs and computer-generated documents. These are related to digital images, and particular areas of difficulty are highlighted. Following this is a glimpse at the various approaches to these difficulties which may be taken in Canada, the United States and the United Kingdom. Finally, some ways in which users of digital image technology might attempt to increase their images' potential for admissibility are summarized.

For the sake of clarity, a couple of points should be made about terminology used in this paper. "Digital images" is used to describe any visual data which may be used by a digital computer, including digital photographs, conventional photographs which have been scanned into a computer, and other visual records such as X-rays, sonograms, infrared images, and so on. The phrase does not include data which are more in the nature of written documents; these are included in the broader category of computer-generated documents or records. Because of the confusion surrounding the term "reliability" when discussing evidentiary principles, the use of this word has been greatly limited, except where some works cited have employed this term. References have instead been made to concepts such as trustworthiness, accuracy and integrity.

II. THE NATURE (AND PROBLEM) OF DIGITAL IMAGES

A DIGITAL IMAGE IS ESSENTIALLY no more than a collection of on/off switches, recorded numerically as a series of binary digits (bits), each digit being either a one or a zero. An electronic sensor (in a digital camera or scanner, for example) typically captures the image by means of many light-sensitive picture elements, or pixels, which are individually turned on or off in order to produce a representation of the subject which may be read by a computer, but not directly by humans. Thus, the visual information is recorded directly as digital data, without creating an analogue representation of the image. The resulting array of data may be intended to represent a "picture" or a written document. The digital image may be stored in the short-term memory of a computer, or it may be re-

corded using a medium of a slightly more permanent nature, such as a floppy disk, hard disk or CD-ROM.[4]

It is clear that both benefits and drawbacks arise from the unique nature of digital images. A digital image can be quickly and easily captured and stored, whereupon it may instantly be viewed, provided the proper computer equipment is available. The digital image exists merely as a recorded collection of computer-readable data, which can be organized into a form that is visually meaningful to a human. There need not, and in the case of digital photographs, probably will not, exist an "original" of the image that is comparable, for example, to a negative of a conventional photograph. In fact, the data that is originally recorded may be easily altered or manipulated, leaving behind no trace of the previously existing file, and no indication that the image was changed since it was first captured. Furthermore, the nature of digital information allows it to be reproduced an infinite number of times as a perfect copy of the original data collection, indistinguishable from it in every way. All of the copies that are made will also be identical to one another, and there will be no degradation of image quality as the copies themselves are reproduced, such as would happen as successive copies of a conventional photo were made.[5] Digital photographs may be printed to look very similar to conventional photographs, but since digital data may be precisely copied at will, one cannot easily distinguish a copy from the original, nor can one be certain which of two images is derivative of the other, if one has been altered in some way.

It is often desirable to be able to easily modify a visual scene or document, and digital images are an attractive option for this same reason. However, the fact that undetectable changes can be made to digital data so readily means that there is a danger that any given digital image portrays something different than did the original image as it was captured, or that the thing which the image depicts never actually existed. Corruption of digital data could occur in a number of ways. First, accidental corruption or destruction of information might result from a digital storage space coming into contact with a powerful magnetic field.[6] Data compression, which is meant to decrease file sizes and conserve data stor-

---

[4] C.A. Guilshan, "A Picture is Worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs Into Evidence" (1992) 18 Rutgers Comp. & Tech. L.J. 365 at 371; R.T. McCarvel, *You Won't Believe Your Eyes: Digital Photography as Legal Evidence* (15 April, 1995) at Part II, Sections 1–2, Available Online: R.T. McCarvel Personal Homepage <http://www.seanet.com/~rod/digiphot.html> (last modified: 11 September 1996); U.K., House of Lords Select Committee on Science and Technology, *Fifth Report—Digital Images as Evidence* (3 February 1998) at para. 1.2 (Box 1), Available Online: U.K Parliament <http://www.parliament.the-stationery-office.co.uk/pa/ld/ldsctech.htm> (last modified 8 May 1998) [hereinafter *Select Committee Report*].

[5] Guilshan, *supra* note 4 at 371-72; McCarvel, *supra* note 4 at Part II, Section 3.

[6] McCarvel, *ibid.* at Part II, Section 3.

age space, could also result in a loss of image details.[7] Secondly, a photographer or another person might intentionally adjust or edit an image for an innocent reason, perhaps simply to make a photograph more aesthetically pleasing. Finally, it is just as plausible that an image could be manipulated with intent to defraud; such changes can be very difficult to detect. While it is true that conventional photographs may also be manipulated, the successful forgery of an analogue photograph generally requires great skill and the use of sophisticated equipment, and there is always an original, apart from the fraudulent version. The original may, of course, be destroyed.

Digital images, on the contrary, can now be readily altered by virtually anyone with a home computer. Any internal inconsistencies in the altered image may be eliminated and replaced, so that there need not be any hint that the image is not an accurate original representation of the thing that it purports to portray. A digital image can be made to look like a conventional document or photograph, and it will thus be very convincing to a viewer, who may be inclined to treat the image as a trustworthy piece of visual evidence.[8] In short, there are a number of factors which contribute to the risk of digital image alteration, and consequently to the risk that a digital image which is sought to be admitted as evidence in court is not altogether trustworthy.

How, then, is a court to be assured that evidence which exists in the form of a digital image is sufficiently trustworthy to be admitted, or to be accorded an influential amount of weight when it forms the basis of a controlling issue in a case? Few would argue that evidence in any form which has probative value on its face should be dismissed out of hand, without conducting an inquiry into whether it meets the applicable standards of admissibility. However, there do not yet exist any statutory rules which directly address the issue of the admissibility of digital images. Consequently, it is arguable that existing evidentiary principles must somehow be drawn upon when considering this issue, so as to avoid the unnecessary exclusion of valuable sources of evidence.[9] Since digital images have characteristics which are comparable to both conventional photographs and to written records stored as computer data, a brief examination of how evidence existing in these two other forms is determined to be admissible may be of assistance in deciding how to assess digital image admissibility.

---

7 D.A. Goodin, *Image Integrity, and the Admissibility of Digital Imaging in Court*, Available Online: TRF Systems Homepage <http://www.trfsys.com/web/lynx/doug_goodin.asp> (last modified 20 November 1998).

8 Guilshan, *supra* note 4 at 374–376; McCarvel, *supra* note 4 at Part II, Section 3.

9 Regarding the importance of admitting all relevant and probative evidence, particularly that available through technological advances, see the reasons of L'Heureux Dubé J. in *R. v. L. (D.O.)*, [1993] 4 S.C.R. 419 at 455.

III. Approaches to Photographs and Computer Data as Evidence

A. Conventional Photographs

A photograph has often been more acceptable in court as evidence than the oral statement of a witness, because of its clear, concise portrayal of an object, scene or event, and its apparently "unassailable accuracy."[10] Frequently cited in Canada with respect to the admissibility of photographs are the three criteria emerging from *R.* v. *Creemer*:[11] a) the photograph's accuracy in representing the facts ("free from distortion and in proper perspective"[12]), b) fairness and the absence of intention to mislead, and c) verification on oath by a person capable of doing so. As is the case for all evidence sought to be admitted, the photographic evidence must also be relevant to a material issue in the case (*i.e.*, it must have probative value and a logical connection to a fact in issue) and its prejudicial effect must not outweigh its probative value—it must not unduly confuse, deceive or mislead the trier of fact.[13]

A photograph or other piece of visual evidence must be properly authenticated in order to be admissible (subject to the consent of the opposing party to admit the evidence without this requirement). Authentication "...is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[14] The normal requirement for authentication is that a capable supporting witness must provide testimony under oath that the evidence is what it is purported to be.[15] For a photograph, this testimony might come from the photographer, or from a witness who can attest that the photo accurately portrays a scene that is familiar to that witness.[16] A difficulty may arise where there has been no human photographer, and there is no witness who can testify that the photograph accurately represents something that the witness has ob-

---

[10] Guilshan, *supra* note 4 at 365–366; Bryant, Lederman & Sopinka, *supra* note 1 at 18.

[11] [1968] 1 C.C.C. 14 (N.S.C.A.).

[12] G. P. Fraser, "Admissibility of Photographic, Film and Videotape Evidence" (1992) 50 Advocate 19 at 22.

[13] E. Goldstein, *Visual Evidence* (Toronto: Carswell, 1991) at 2-14, 2-15; the general standard for admissibility of photographic evidence in the United States is set out in Fed. R. Ev. 401, 402 (relevancy) and 901 (authentication).

[14] Fed. R. Ev. 901(a).

[15] Fraser, *supra* note 12 at 22; D. Paciocco & L. Steusser, *The Law of Evidence* (Concord, Ontario: Irwin Law, 1996) at 238; in the United States, the authentication requirement is set out succinctly in Fed. R. Ev. 901(a).

[16] Paciocco & Steusser, *ibid.* at 240.

served. In such a situation, the nature of the authentication procedure may be different: the evidence may still be readily admissible provided that an explanation is given of the technique used to produce the image, in addition to evidence respecting the "reliability of the technical apparatus" that was employed.[17]

Typically, the authentication standards applied by the courts to photographic evidence are quite liberal, and it is normally sufficient to have a supporting witness testify that a photograph accurately represents what it is supposed to represent.[18] Nevertheless, "...what is required in testimony to establish the admissibility of the photograph will vary according to how the photograph came into being and what it is intended to prove."[19] In some circumstances, the "chain of custody" rule might be invoked as a further authentication requirement, by which a party may need to clearly establish who had the evidence in possession from the time it was created to the time it was sought to be admitted into court. It will therefore be helpful, though seldom necessary, for proponents of such evidence to have the circumstances surrounding its origin precisely documented.[20] Of course, where the authenticity of a piece of evidence is challenged, the trier of fact will need to make the ultimate decision on this matter.

There are two primary bases for the admissibility of visual evidence such as photographs and videotapes: the illustrative (or pictorial testimony) theory and the silent witness theory. Under the illustrative theory, a photograph, videotape or motion picture is linked to the testimony of a witness, and it has no probative value independent of the testimony with which it is associated. It is considered to be "pictured communication" of a qualified witness, and may only be used to support or supply detail to the oral testimony; a sponsoring witness is required to testify that what is shown in the image is an accurate reflection of that which was observed in person.[21] Photographs and other visual evidence that is admitted under the silent witness theory, on the other hand, is said to be self-authenticating and to speak for itself, as substantive evidence that a thing existed at one time as it is portrayed in the evidence. Under this theory, an eyewitness need not testify about authenticity, but testimony will still be required from some qualified person that the representation is true and accurate.[22]

---

17 *Greenough* v. *Woodstream Corp*, [1991] O.J. No. 77 (Ont. C.J. Gen. Div.).

18 Fraser, *supra* note 12 at 22; Guilshan, *supra* note 4 at 368.

19 Fraser, *ibid.* at 22.

20 *Ibid.*

21 *Ibid.* at 21; Goldstein, *supra* note 13 at 2–4; Paciocco & Steusser, *supra* note 15 at 240–241.

22 Fraser, *ibid.* at 21; Goldstein, *ibid.* at 2–6; Guilshan, *supra* note 4 at 368–369.

B. Computer-Generated Records

Case law that is pertinent to the topic of the admissibility of computer data as evidence is surprisingly sparse, despite the present ubiquity of computer based record-keeping systems.[23] The difficulties surrounding the character of computer data and the fact that it may be so easily manipulated apparently make the construction of evidential rules in this area a difficult task for the courts. However, computer data is often admitted under the business records exception to the hearsay rule, which was developed at common law and is now supplemented or replaced by statute.[24] While this exception was developed with paper documents in mind, the analogy between paper records and computer-generated records is easily drawn in this context, and the exception is therefore adaptable.[25] In addition, business records are said to be admitted because of their trustworthiness as indicated by the reliance of a business upon them, and this does not depend upon the medium or format in which the records exist.[26]

The business records exception allows the admission of records which are kept in the ordinary course of business. Business records are normally admitted only when they have some degree of trustworthiness, which is produced by such factors as "...systematic checking, by regularity and continuity which produce habits of precision, by the actual experience of business in relying upon them, or by a duty to make an accurate record as part of a continuing job or occupation."[27] The truth of the actual contents of the record need not be proven, under the business records exception; in theory, the fact that a record was created and relied upon in the course of business provides enough proof in this respect to support the admission of the record.[28]

Business records, as documentary evidence, must be properly authenticated. A party which seeks to make use of the business records exception to the hearsay rule in order to admit computer-generated records (as appears to be the

---

23 But see *R. v. Hall*, [1998] B.C.J. No. 2515 (B.C.S.C.) [hereinafter *Hall*], as one recent case which contains a thoughtful discussion of admissibility rules as applied to computer records.

24 See *e.g. Canada Evidence Act*, R.S.C. 1985, c. C-5, s.30; in the United States, see Fed. R. Ev. 803(6); *Hall*, *ibid.* at paras. 53–65.

25 J.D. Ewart, *Documentary Evidence in Canada* (Toronto: Carswell, 1984) at 67; S.A. Kurzban, "Authentication of Computer-Generated Evidence in the United States Federal Courts" (1995) 35 IDEA 437 at 441–442; McCarvel, *supra* note 4 at Part III, Section 2.

26 Kurzban, *ibid.* at 459.

27 *Advisory Committee's Note*, 56 F.R.D. 183, 307 (1974), cited in McCarvel, *supra* note 4 at Part III, Section 2; see also Ewart, *supra* note 25 at 45–47.

28 *Hall*, *supra* note 23 at para. 65; Uniform Law Conference of Canada, *Uniform Electronic Evidence Act – Consultation Paper* (March 1997) at para. 53, Available Online: The University of Alberta Faculty of Law <http://www.law.ualberta.ca/alri/ulc/current/eelev.htm> (last modified 17 April 1997) [hereinafter *ULCC Consultation Paper*].

norm) will need to establish the authenticity of that evidence by leading foundational proof of the accuracy and trustworthiness that is expected of a business record. Unless an inference of authenticity can somehow be made, testimony about the record, the circumstances surrounding its entry, processing and storage, and the record-keeping system itself should be made available, so that a finding that the record is trustworthy can be supported (though trustworthiness may have more impact on a record's weight than its admissibility).[29] Logically, the satisfaction of the authentication requirement is precisely what will allow a record to be admitted under the business records exception to the hearsay rule, since accuracy and trustworthiness must necessarily be inferred from evidence relating to the entire system of record production and storage, including the fact that the record was generated and relied upon in the regular course of business.

The amount of supporting evidence necessary to meet the authentication requirement will depend upon the type of record that is sought to be admitted, and how much reliance is to be placed upon it.[30] Even though courts, in exercising their discretion, do not often strictly enforce foundational requirements for authentication, it is advisable that the proponent of the evidence be ready to supply the information that may be needed, such as details about the computer system which has generated the evidence. In this way, the proponent can possibly avoid the risk that a challenge to authenticity may result in an unfavourable exercise of the court's discretion, and ultimately in the exclusion of the evidence.[31]

IV. BEST EVIDENCE RULE

AT COMMON LAW, WHERE DOCUMENTARY evidence is offered for its truth and it forms the basis of a controlling issue in the case, it is necessary for the proponent to satisfy the best evidence rule, which requires that the original of a document be tendered, if available.[32] The rule, which provides a way to safeguard the integrity of documents and ensure that they have not undergone changes before being submitted as evidence, has been largely displaced by various statutory and common law exceptions. A flexible approach to the best evidence or original documents rule is now advocated, so as not to restrict the admission of evidence which has potential for advancing the truth in an issue; it is

---

29 R.A. Bain & C.A. King, "Comment: Guidelines for the Admissibility of Evidence Generated by Computer for Purposes of Litigation" (1982) 15 U.C. Davis L.R. 951 at 954–956; Ewart, *supra* note 25 at 68–69; Kurzban, *supra* note 25 at 443–445; *Hall*, *ibid.* at paras. 61–64; see the discussion on weight *infra* note 37 and accompanying text

30 Bain & King, *ibid.* at 958.

31 *Ibid.* at 962.

32 Paciocco & Steusser, *supra* note 15 at 242–243.

desirable that the best available evidence be secured, but not that evidence having probative value will be unduly excluded.[33] Though the rule seems to have fallen out of use, the idea that records submitted as evidence ought to have identifiable originals apparently continues to subsist.[34]

Direct application of the best evidence rule becomes problematic when an attempt is made to determine what the original of a computer-generated record is. As discussed above in the consideration of the character of digital images, the concept of an original data record is, to a large extent, meaningless. Nonetheless, the underlying basis for the best evidence rule has obvious application to computer-generated evidence in general, since there are numerous opportunities for errors to arise in the entry, processing, storage and reproduction of data.[35]

Courts have struggled to fit computer-generated documents within a rule that is better suited to paper documents, by going through "semantic contortions" such as defining a computer's memory as a record, and classifying computer printouts as originals. These manoeuvres seem to defeat the purpose and rationale of the best evidence rule, hence the many calls for shifting the focus of the rule away from the concept of an original, where the admissibility of computer-generated documents is in issue.[36]

V. WEIGHT

NO MATTER THE FORM OR CHARACTER of the evidence, once it is admitted the trier of fact will still have discretion as to the amount of weight it will be given. Obviously, the evidence will be no more trustworthy than the witness who is verifying its authenticity. Many of the same factors which are relevant to a demonstration of a record's trustworthiness and thus to its admissibility, such as details about the record-keeping system, will also potentially have bearing upon a determination of the weight to be given to the evidence. Since it is not desirable or practical that the same supporting evidence should be submitted at both stages, it must be decided whether the primary inquiry into trustworthiness should be performed at the admission stage, or whether a low standard for admissibility should be set, with evidence relating to a record's trustworthiness be-

---

[33] D. Bender, *Computer Law: Evidence and Procedure* (New York: Matthew Bender, 1982) at 5-50; *R. v. Betterest Vinyl Manufacturing Ltd.* (1989), 52 C.C.C. (3d) 441 (B.C.C.A.).

[34] H. Stewart, *Some Thoughts on Computer-Generated Evidence* (June 1996) at paras. 22–23, Available Online: The University of Alberta Faculty of Law <http://www.law.ualberta.ca/alri/ulc/96pro/e96b.htm> (last modified 25 March 1997).

[35] Bender, *supra* note 33 at 5–50.

[36] *Hall*, *supra* note 23 at para.52; Stewart, *supra* note 34 at para. 22; *ULCC Consultation Paper*, *supra* note 28 at paras. 22–29.

ing more important when deciding upon the weight to be accorded.[37] It is not proposed that this question be dealt with in detail here, but it ought to be flagged as an issue which merits consideration.

VI. APPLICATION TO DIGITAL IMAGES

DIGITAL IMAGES HAVE CHARACTERISTICS which cause them to differ in certain respects from both conventional photographs and other forms of computer-generated evidence. Therefore, the application to digital images of admissibility rules pertaining to these other two types of evidence does not completely satisfy the concerns which have been raised.

It is important to distinguish digital images from conventional photographs, because the trust that has been traditionally placed in the latter cannot be properly placed in the former. Because of the nature and characteristics of digital images, their accuracy and trustworthiness will always be suspect, in the absence of some unassailable guarantee of integrity. A dilemma arises when deciding under which of the two traditional bases for admitting a conventional photograph a digital image should be admitted. On one hand, the silent witness theory is problematic because undetectable changes to digital images are so easily made, and therefore it makes little sense to allow such evidence to be self-authenticating. On the other hand, situations will frequently arise in which there is no photographer or witness who can confirm that a digital image accurately reflects a scene that was observed, and so this evidence will not be admissible under the pictorial testimony theory.[38] It may be necessary to reformulate the bases for admissibility slightly to account for the peculiarities of digital evidence.

Certain of the criteria for admissibility which are applied to conventional photographs can be rationally utilized to test the admissibility of digital images. For instance, a determination must still be made that the evidence has probative value which is not outweighed by its prejudicial effect. The rules requiring fairness and accuracy in representing the facts also remain applicable, though the amount or degree of supporting evidence needed to prove these elements could vary depending on the form in which the evidence exists.

In the context of digital images, there are at least two difficulties which arise when attempting to apply the standard of authentication which is employed for conventional photographs. The first problem has already been mentioned: there will often be no witness who is capable of testifying about the identity of an image. The second problem is that even if there is a photographer or corroborating

---

[37] *ULCC Consultation Paper*, *ibid.* at para. 30.

[38] H.J. Onsrud, *Evidence Generated from GIS*, Available Online: University of Maine <http://www.spatial.maine.edu/GIS_Evidence.html> (last modified 19 July 1995).

witness available, oral testimony in support of the integrity of the image will probably not be sufficient to guarantee authenticity. This, again, is because changes to digital images can be so subtly and easily made, and the memory of a witness may not be dependable enough to allow alterations to an image to be detected. Furthermore, any earlier versions of the image that existed may have been erased, outside of the knowledge of the witness. If legal rights or liabilities depend on the particular material elements of a scene, then courts may well require some other assurance that there has been no tampering with an image.

The standard of authentication which is applied to other forms of computer-generated evidence is perhaps more promising than that for photographs. Evidence about the system used to generate, process, store and reproduce a digital image is likely to be available even in the absence of a photographer, and this test does not rely so heavily upon the memory or knowledge of a live witness with respect to an individual image. Still, something more than evidence supporting the integrity of the record-keeping system may be desired to assure a court that a particular digital image is accurate and trustworthy, especially because of the heavy impact which evidence in photographic form can have on the minds of triers of fact.

There are also limitations in treating digital images as though they fall within the ambit of the business records exception to the hearsay rule, like some other forms of computer-generated records. For one thing, the hearsay rule is normally applied only to out-of-court statements or assertions. It is doubtful that a reproduction of a digital image which looks like a photograph can always be construed as a statement; this would be stretching the definition of "statement" beyond its logical limits. Secondly, one of the primary criteria for the admissibility of business records is that they have been kept in the ordinary course of the dealings of a business or enterprise. While the definition of "business" is typically interpreted very broadly,[39] the use of computers and of digital image technology is very extensive and by no means confined to the realm of business; digital images which have evidential value but which cannot be characterized as having been recorded in the ordinary course of business are bound to come before the courts. Assuming the hearsay rule does apply, proponents of these images may have to look to another exception to have them admitted as evidence. Thirdly, business records are deemed to be trustworthy because of the reliance of a business upon them, and this is often the primary basis for their admissibility. It is arguable that the reliance of a business upon a digital image which forms part of its records is not, by itself, sufficient assurance that such a record is worthy of trust. Notwithstanding these possible difficulties with the application of the business records exception to digital images, the authentication principles

---

[39] I. Younger, "Computer Printouts in Evidence: Ten Objections and How to Overcome Them" in American Bar Association, *A.B.A. Litigation Manual* (Chicago: A.B.A., 1983) 204 at 204.

which are applied to business records may still prove to be useful in formulating admissibility standards for digital images.

The best evidence rule is even more unhelpful in assuring the accuracy or integrity of a digital image. While originals are generally preferred to copies under this rule, the copies of an original digital image can conceivably be more accurate than the image from which they are derived. Furthermore, a printout of a digital image is hardly a move toward accuracy, and it is certainly not closer to the original image, whatever that might be. A conventional photograph may be accepted as an original because of its physical connection to the negative from which it came, but a printout of a digital image does not have such a strong link with the original data as recorded. Regardless, the basis underlying the establishment of the best evidence rule, namely to safeguard against illicit alterations to records sought to be admitted as evidence, is certainly applicable in the context of digital images.

VII. RESPONDING TO THE PROBLEM

A. Canadian Approach

The Uniform Law Conference of Canada ("ULCC") has been examining the evidentiary problems surrounding computer-generated evidence for several years, with the ultimate goal of creating uniform rules of evidence for the acceptance of electronic records by courts. In August 1997, the ULCC approved draft legislation entitled *Uniform Electronic Evidence Act* ("*UEEA*").[40] Following this event, legislation was tabled in Parliament which also contains provisions specifically dealing with the admissibility of electronic documents. Known as the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), Bill C-54 received first reading on 1 October 1998.[41] The amendments to the *Canada Evidence Act* ("CEA") within the Bill closely resemble the ULCC's proposals in the *Uniform Electronic Evidence Act*.

1. Hearsay

Assuming that the rule against hearsay does have application against the various types of electronic records, including digital images, it does not seem as though these new forms of evidence pose a serious problem when confronting the rule. This is true especially as the common law in Canada has been moving

---

[40] An amended version of the draft legislation was produced in September 1998, Available Online: The University of Alberta Faculty of Law <http://www.law.ualberta.ca/alri/ulc/acts/eeeact.htm>

[41] Bill C-54 became Bill C-6 with the 2nd Session of the 36th Parliament in 1999, receiving first reading on 15 October 1999.

toward a principled approach to hearsay in cases such as *R.* v. *Smith*[42], under which hearsay may be admitted where it is shown to be necessary and reliable, and its probative value is not outweighed by its prejudice in the eyes of the court. Furthermore, electronic records can frequently fall within the business records exception or another exception to the hearsay rule (subject to the concerns which have been raised earlier), whether under statute or the common law; it is arguable that the medium of the record sought to be admitted is not important to this issue.[43] Consequently, neither the *UEEA* nor the *PIPEDA* contains provisions which contemplate changes to the existing law relating to hearsay. Indeed, it is important to note that the proposed legislation does not affect any existing law relating to the admissibility of documents except the authentication and best evidence rules, as stated in s.2(1) of the *UEAA*, and in s.31.7 of the proposed amendments to the *CEA*, in *PIPEDA* s.56.

2. Authentication

Canadian commentators appear to agree that computer-generated evidence ought to be subject to authentication requirements that are similar to, or perhaps even more stringent than those for paper documents, since for both types of records there exist concerns regarding the possibility of alteration and forgery.[44] Given the character of computer-generated records and the difficulty of producing proof of the trustworthiness of an individual record (especially of a digital image), it has been suggested that the proponent of such evidence, in establishing authenticity, should bring evidence relating to the integrity of the record-keeping system through which the record was produced, rather than the specific record itself. [45] However, the ULCC has stressed that the authentication test is to be one of "identity and not integrity."[46] Therefore, "the proponent needs only to bring evidence that the record is what the proponent claims it is" at the authentication stage, where the evidence would, of course, be open to oral cross-examination.[47] The proposed legislation contains provisions which

---

[42] (1992), 75 C.C.C. (3d) 257 (S.C.C.).

[43] *ULCC Consultation Paper*, *supra* note 28 at paras. 51–58; Stewart, *supra* note 34 at para. 24; E.A. Tollefson, "Computer-Produced Evidence in Proceedings Within Federal Jurisdiction" (in Appendix N to the 1995 Proceedings of the Uniform Law Conference of Canada) (August 1995) at para. 106, Available Online: The University of Alberta Faculty of Law <http://www.law.ualberta.ca/alri/ulc/95pro/e95n.htm> (last modified 25 March 1997).

[44] Stewart, *ibid.* at 10.

[45] *Ibid.*; *ULCC Consultation Paper*, *supra* note 28 at para. 17.

[46] *ULCC Consultation Paper*, *ibid.* at para. 17.

[47] Canada, Uniform Law Conference of Canada, *Uniform Electronic Evidence Act* (September 1998) at Section 3, Available Online: The University of Alberta Faculty of Law <http://www.law.ualberta.ca/alri/ulc/acts/eeeact.htm> [hereinafter *ULCC Comments*].

reflect this approach to the authentication requirement, in *UEAA* s.3 and *PIPEDA* s.56 (proposed *CEA* s.31.1). Only after the computer-generated evidence has passed the low-barrier authentication requirement would it be subject to attacks on its accuracy or integrity in the next stage of the admissibility inquiry, which is presented by the ULCC as a "new best evidence rule."[48]

3. *Best Evidence*

Clearly, the best evidence or original document rule has little practical application in the context of computer-generated documents, since the concept of an original data record is substantially devoid of meaning. There is an argument to be made that "[a] statutory regime appropriate to computer-generated records would merge the "original document" rule with the problem of authentication."[49] It has also been proposed that the purpose of the best evidence rule, to protect the document from errors and alterations and to ensure its integrity, could be met through a reformulation (or displacement) of the existing best evidence rule for the special situation of computer records.[50] The focus of proof for this new formulation of the rule would be not on the integrity of the record itself, but on the security and trustworthiness of the system that produced the record.[51] Proving the integrity of the system would thereby prove the integrity of the record in whatever form it may be presented.[52]

In s.4 of the *UEEA* and s.56 of the *PIPEDA* (proposed *CEA* s.31.2), it is stated that, for electronic documents, the best evidence rule will be satisfied "on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored." Additionally, a printout of an electronic document will satisfy the new best evidence rule if it "has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout." *UEEA* s.5 and proposed *CEA* s.31.3 set out what is described in the marginal notes as a presumption of integrity in favour of the system by which the record is produced and stored. This presumption, which is rebuttable by contrary evidence from an opponent, may arise if foundation evidence is presented by the proponent in three alternative areas. First, evidence may be given that the computer system through which the electronic evidence was generated was working properly at all material times, or that if it

---

[48] *Ibid.*

[49] Stewart, *supra* note 34 at para. 23.

[50] *ULCC Comments*, *supra* note 47 at Section 5.

[51] K. Chasse, "Computer-Produced Records in Court Proceedings" (in Appendix J to the 1994 Annual Meeting of the Uniform Law Conference of Canada) (June 1994) at para. 46, Available Online: The University of Alberta Faculty of Law <http://www.law.ualberta.ca/alri/ulc/94pro/e94j.htm> (last modified 25 March 1997).

[52] *ULCC Consultation Paper*, *supra* note 28 at para. 26.

was not working properly, this fact did not negatively affect the integrity of the document adduced, and there is no other reason to doubt the integrity of the system. Secondly, it may be established that the electronic evidence was recorded or stored by a party to the proceedings other than the proponent (the *PIPEDA* specifies that the party must be adverse in interest to the proponent). Thirdly, evidence may be led that the document in question was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings.

According to the ULCC, these provisions are designed to set out the basic criteria for a simple test of reliability, which may be met by evidence "brought by anyone and about anyone's records."[53] Again, it appears that reliability is established once a fairly low threshold of proof is met, whereupon the challenging party is capable of bringing evidence that the electronic record is unreliable, in order to rebut the presumption. The low standard is desirable in order to avoid putting unnecessary burdens of time and expense on the proponents of electronic records which are unlikely to be challenged. Of course, there is a balance to be reached here, between allowing litigants to avoid inconvenience and expense, and giving opponents a reasonable opportunity to challenge the integrity of an electronic record.[54] Presumably, additional evidence could be brought by the proponent to satisfy the court of the record's integrity, if a legitimate challenge is brought by the opponent, or if the court has concerns in this area. The question of what the onus on the opponent is to rebut the statutory presumption of integrity appears to have been left open.[55] The ULCC has also considered other options for the best evidence rule which have been suggested by commentators, such as the requirement that legislation should specify that certain record-keeping standards must be complied with, or that proponents of electronic records must provide an opponent with notice in advance of an intention to produce such records as evidence. However, these options are seen to place unnecessarily expensive and burdensome barriers in the way of proponents.[56]

While the *UEEA* and the *PIPEDA* do not specify that any particular procedures, rules or standards are to be adhered to or followed in recording or storing electronic documents, ss. 6 and 56 (proposed *CEA* s.31.5), respectively, make it relevant to the court's consideration of system reliability whether the record-keeping system has adhered to any particular "standard, procedure, usage or practice" in recording and storing the documents. Furthermore, this adherence to a particular standard will be considered in light of the type and purpose of

---

[53] *ULCC Comments*, *supra* note 47 at Section 5.

[54] *ULCC Consultation Paper*, *supra* note 28 at paras. 31–38.

[55] *Ibid.* at paras. 44–46.

[56] *Ibid.* at paras. 40–42.

the record which is sought to be admitted, and the type of business from which the record was produced. This gives records managers broad discretion as to whether to establish and follow their own record-keeping standards, or to follow other external standards which have been established or endorsed by a particular industry (such as Geographic Information Systems). By way of example, one well-recognized standard is entitled *Microfilm and Electronic Images as Documentary Evidence—CAN/CGSB11.72-93*, developed by the Canadian General Standards Board; it is currently used by regulatory bodies such as Revenue Canada.[57] Relevant standards are also being produced by such international bodies as the International Standards Organization.

Evidence to support the statutory presumption of reliability may be presented by affidavit or orally, if desired, in accordance with *UEEA* s.7 and s.56 of *PIPEDA* (proposed *CEA* s. 31.6). The *PIPEDA* also allows the cross-examination of the deponent as of right, if the deponent is an adverse party or is under the control of an adverse party, and with leave of the court in any other case.

Some of the approaches taken by the proposed changes to the *Canada Evidence Act* in the *PIPEDA* are not without precedent in Canadian legislation. For instance, articles 2837–2839 of the *Quebec Civil Code* (applying to "data respecting a juridical act") presume the reliability of data records for purposes of admissibility, provided that evidence is brought respecting the reliability of the record-keeping system. The presumption also applies to the records of third parties, on proof that the data were entered as part of an "enterprise." Recent amendments to the New Brunswick *Evidence Act* [58] respecting electronically stored documents also imply that evidence about the reliability of the computer system will be required to establish the integrity of the computer record. The New Brunswick statute adds an additional condition for admissibility, namely, that the paper original of an imaged document must have been destroyed; this would seem to limit the rule's usefulness somewhat.

4. A *Summary of the* Canadian Approach

The approach taken by the proposed Canadian legislation is consistent with the idea that the law should move away from thinking about electronic records in the same terms as paper documents, which may exist as originals and as copies. Instead, it is preferred that evidentiary rules specific to computer-generated documents be enacted, which focus more pragmatically on whether the intentions of those producing such documents are accurately reflected in the format in which the documents are presented, and whether the documents can be shown to be reliable through evidence of the reliability of the system which pro-

---

[57] V. Gurushanta, *Canada's Uniform Electronic Evidence Act—It's Finally Here!*, Available Online: <http://www.ciims.ca> (last accessed 12 April 1999).

[58] R.S.N.B. 1996, c.52.

duced them. Because of the dynamic nature of computer technology, it is desirable that the law be accommodative to new forms of evidence and flexible enough to allow for the growth of technology, but also that it provide for some scrutiny of challenged records, where warranted.[59]

B. American Approach

1. Hearsay

From the apparent focus of many of the scholarly articles which discuss the admissibility of computer-generated evidence, it seems that federal and state courts in the United States tend to treat records of this type as falling within the business records exception to the hearsay rule. As already discussed, there are complications involved in the application of the hearsay rule and the business records exception to many of the forms in which computer-generated evidence now manifests itself. Nevertheless, many writers continue to express confidence that the business records exception, where applicable, is capable of handling reliability and accuracy problems, "with a few modifications."[60] Under R. 803(6) of the Federal Rules of Evidence, a data compilation (or other record) will not be excluded by the hearsay rule if it was made relatively contemporaneously with the event to which it relates, by a person with knowledge of the event, as an activity conducted regularly in the course of business. The rule contains the additional safeguard that the record may still be excluded if the "source of information or the method or circumstances of preparation indicate lack of trustworthiness... ." Stated this way, the foundational requirements of the business records exception appear to be rather stringent when applied to computer-generated evidence, and there are presently conflicting opinions on whether the standard should be set even higher, or whether triers of fact should be given greater discretion as to the weight to be accorded to the evidence, following a low threshold of admissibility.[61] In contemplating the foundational requirements of the business records exception, the discussion must of necessity flow into a consideration of the authentication requirement, for the foundation needed for authentication is essentially that which will satisfy the exception to the hearsay rule.

2. Authentication

As suggested above, there has been a variety of proposals put forward as to how strict the foundational requirements ought to be for computer-generated evi-

---

[59] ULCC *Consultation Paper*, *supra* note 28 at paras. 77–79; Stewart, *supra* note 34 at para. 26.

[60] R. Snyder, Note, "Assuring the Competency of Computer-Generated Evidence" (1989) 9 Comp. L. J. 103 at 121.

[61] Onsrud, *supra* note 38.

dence in general, and digital images in particular. Because of the virtual impossibility of guaranteeing the integrity of certain types of digital records, some commentators feel that the probative value of such evidence could not possibly outweigh its potential prejudicial effect, and the admissibility of computer-generated records should be denied outright.[62] Others, believing computerized record-keeping systems to be inherently trustworthy, prefer to set a very low standard to be met in establishing the foundation needed to prove authenticity, giving the trier of fact broad discretion as to the degree of accuracy, trustworthiness and ultimately weight to accord to the computer-generated evidence adduced.[63]

Advocates of the strict approach to authentication favour the setting of high standards to be met by foundation evidence. Accordingly, an authenticating witness would need to prove more than simply that a record was kept in the regular course of business, contemporaneously with its corresponding event. Beyond this, the witness might be required to provide detailed testimony about the system used to produce and store the record, including the software package utilized and input procedure and controls used to assure data accuracy. Additionally, the witness might have to testify about where possible errors could have crept into the system, and why such errors are unlikely to be present or why they have not had a significant impact upon the accuracy of the record. One writer thinks it advisable to establish foundational requirements relating to the trustworthiness of computer software, especially software which is not widely used or has been created specifically for a particular enterprise.[64] A recommended remedy for the prejudicial effect of computer-generated evidence, the trustworthiness of which is dubious, is to require disclosure by a party to an opponent of the intent to use such evidence, so that the opponent could "educate" the trier of fact on the shortcomings of the evidence, and thereby attempt to alleviate some of its potential damage. In the absence of timely disclosure, the judge might exclude the evidence entirely, if it is seen as more prejudicial than probative.[65]

Christine Guilshan has written one of the few articles which discusses the evidentiary problems specifically surrounding digital photographs. Her argument in favour of a strict approach to the authentication of digital photographs is that only the actual photographer of a digital photograph should be permitted to be the sponsoring witness of the evidence. The photographer would need to testify

---

[62] J.L. Dartley, Note, "Lost Horizons?: Tortious and Philosophical Implications of Computer Imaging" (1993) 19 Rutgers Comp. & Tech. L.J. 199 at 215; McCarvel, *supra* note 4 at Part IV.

[63] Onsrud, *supra* note 38.

[64] Snyder, *supra* note 60 at 107–111.

[65] *Ibid.* at 120.

that the photo is what it appears to be, and has not been manipulated. If the photographer is unavailable or is unable to testify to the integrity of the image (or where there is no photographer), the digital photograph would be denied admissibility under this theory.[66] In support of her proposed approach, Guilshan stresses the importance of safeguarding against image manipulation. She allows that hers is a very stringent standard to be reached, but counters that it is the safest way to ensure image integrity, and it still allows for some admissibility of digital photographs. She sees the alternative as being the rejection outright of such evidence, which, she concedes, would be entirely too drastic and impractical. Guilshan contends that it is no longer safe to rely solely upon evidence pertaining to the reliability of the computer system through which a digital photograph is produced, since the manipulation of digital photographs is so easily accomplished and is often undetectable. Furthermore, she states that the "silent witness" or "pictorial testimony" theory of admissibility for photographic evidence should be displaced with respect to digital photographs, by authenticating measures other than self-authentication.[67] Finally, the suggestion is made that perhaps courts at the appeal level could be allowed a greater scope of review of trial courts' discretionary decisions regarding the admissibility of digital photographs, and of their findings on relevance and authentication, as another means of shielding litigants from the risk of prejudice that is inherent in digital photographs.[68]

Concern about the trustworthiness of computer records in general has prompted some to express the opinion that the statutory law of evidence should be altered somehow in order to accommodate these new forms of evidence. While the use of computer technology has now become quite widespread and familiar to the average person, one older article suggests that the Federal Rules of Evidence should be changed to require that substantial foundation testimony be brought about the reliability of computer records so that the evidence could be intelligently weighed, since opponents and triers of fact were unlikely to understand data processing sufficiently to comprehend the problems surrounding computer-generated evidence.[69] Instead of modifying the Federal Rules of Evidence, another option proposed is that a separate comprehensive statute could be enacted to deal with the admission of computer-generated evidence, as some other countries have done.[70] It has even been argued that uniform international legal standards respecting the admissibility of computer records should be

---

66 Guilshan, *supra* note 4 at 378–379.

67 *Ibid.* at 379.

68 *Ibid.*

69 P. N. Singer, "Proposed Changes to the Federal Rules of Evidence as Applied to Computer-Generated Evidence" (1979) 7 Rutgers J. of Comp. & Tech L.J. 157 at 193.

70 Younger, *supra* note 39 at 204–207.

drafted and followed, because of the problems that may arise from inconsistencies between states in the treatment of evidence.[71]

Notwithstanding the suspicion voiced by many about the trustworthiness of computer-generated evidence, satisfaction with the capability of the Federal Rules of Evidence of accommodating the authentication of new forms of evidence has been expressed, though it is allowed that technological advances could easily make existing rules obsolete.[72] In fact, one writer believes that the tendency of the courts to require a competent foundational witness to testify about the facts within a computer record and about technical aspects of the record-keeping system (including the computer itself) is too burdensome on those needing to rely upon computer records. On the contrary, the writer advocates that judicial notice should be taken of computers' accuracy, since computerized systems of record keeping are no less trustworthy than "conventional" systems. This would result in a presumption of integrity of a computer-generated record once it is shown to qualify for admission under a hearsay exception, for example. It follows that a witness would not have to establish an extensive and technical foundation as a prerequisite to admissibility, but would only need to testify to authenticity (that the record is what its proponent claims, under Fed. R. Ev. 901), as well as the record's status and qualifications under a hearsay exception, as necessary.[73]

Another commentator's extensive consideration of the authentication requirement also leads him to believe that existing standards probably exceed the standard that is needed. He states that "jurists' unease with computers" prompts their "concern for standard equipment, reliable operation, correct repair, and the use of error-resistant procedures" in the creation and storage of computer records.[74] The writer's view is that computer-generated evidence ought to be considered no less worthy of trust than evidence on paper, and that existing evidentiary rules are presently sufficient for dealing with computer records. In particular, he asserts that the authentication standards for business records stored on a computer ought to be lower than for other types of computer-generated evidence, because of the unlikelihood that someone would have enough to gain, in addition to sufficient skill and access to the system, from altering individual records. Of course, the authentication standard could be var-

---

71 A.H. Boss, "The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies" (1991) 46 Bus. Law. 1787; K.J. Kotch, "Addressing the Legal Problems of International Electronic Data Interchange: the Use of Computer Records as Evidence in Different Legal Systems" (1992) 8 Temple Intl. & Comp. L.J. 451 at 452.

72 Kurzban, *supra* note 25 at 451; P.M. Storm, "Admitting Computer Generated Records: A Presumption of Reliability" (1984) 18 John Marshall L.R. 115 at 125–129, 147–149.

73 Storm, *ibid.* at 147–153.

74 Kurzban, *supra* note 25 at 453.

ied, depending upon the value of the data in question and the likelihood that accidental or malicious harm could befall it.[75]

3. *Best Evidence In the United States*

The best evidence rule continues to focus on the concept of an original as distinct and somehow more trustworthy than a copy of a record. The characterization in the Federal Rules of Evidence of any accurate printout or "output readable by sight" as an "original"[76] for the purposes of the rule means that the rule is not an effective barrier to admissibility, nor does it provide any assurances about the integrity of a digital record.[77] The best evidence rule has consequently not been treated as significant in much of the discussion of the difficulties associated with the admission of computer-generated evidence.

4. *A Summary of the American Approach*

Many American writers express their confidence in the ability of existing rules of evidence to accommodate the admissibility problems which surround computer-generated documents, with few difficulties. Unfortunately, much of the discourse on this topic addresses the admissibility of computer records generally, and does not consider the unique qualities of digital images, which set them apart in important respects from records which are comparable to written documents. The few recent articles which focus specifically on the evidentiary problems of digital images do reveal concern about the inadequacy of existing doctrines.[78] This is an area of law in which it is vital that the scholarship be as contemporary as possible, given the rapid pace of technological change today.

The hypothesis might be made that the inevitable proliferation of digital image production and use will prompt greater scrutiny of the admissibility issues which have been raised, and will eventually cause practical steps to be taken in the way of establishing relevant rules or standards, in the interests of certainty and clarity. Alternatively, such standards could be developed more gradually through the courts, though this is likely to result in the adoption of widely varying approaches to this matter by different jurisdictions.

C. United Kingdom Approach

It may be helpful to take brief notice of the direction in which the United Kingdom could be proceeding with respect to the admission of digital images in the courts, as discussed in a recent report from a Select Committee of the House of

---

[75] *Ibid.* at 452–453.

[76] Fed. R. Evid. 1001(3).

[77] Bender, *supra* note 33 at 5-57–5-59; McCarvel, *supra* note 4 at Part III, Section 3.

[78] See *e.g.* Guilshan, *supra* note 4; McCarvel, *supra* note 4; Onsrud, *supra* note 38.

Lords.[79] According to the report, while there currently exists no legislation which specifically addresses digital images used as evidence, existing law which deals with comparable forms of evidence such as "technological recordings" can be applied to digital images, since digital images are not seen as fundamentally different.[80]

In the UK, the hearsay rule is apparently not a barrier to the admissibility of digital images, for two reasons. First of all, "information captured by a recording device," such as videos and still images, is not defined as hearsay, and is therefore not excluded by the rule.[81] Secondly, the hearsay rule has been abolished in civil proceedings by legislation which also allows a copy of a document to be admitted (regardless of whether an original exists) and automatically admits documents which are part of the records of a business.[82] Thus, it seems that digital images will be easily admitted in civil proceedings, though the judge before whom the evidence is presented will have substantial discretion to determine the probative value to be attached, which is largely a function of the degree to which the authenticity of the image is proven.[83] It should be noted that the barrier to the admissibility of computer records is somewhat higher in criminal proceedings, where the reliability of the computer system through which the record was produced must be proven and certified.[84]

A party who offers a digital image as evidence will probably have to satisfy the court that the image is authentic, through further evidence about the origin of the image, and whether or how it has been altered since its production.[85] More weight will be given to an image which is authenticated to a high degree, and various factors will assist in satisfying the court of the record's authenticity. An audit trail which describes what has happened to the record, from the time the image was originally captured to the time a copy was offered as evidence, will be highly favoured in this regard. Evidence respecting the record-keeping system itself, especially of compliance with approved image storage standards and of security precautions taken against tampering could aid authentication and give more weight to the image that has been adduced. Finally, features which are "embedded" in the image itself, such as digital signatures and water-

---

79 *Select Committee Report*, *supra* note 4.

80 *Ibid.* at para. 2.14.

81 *Ibid.* at para. 2.15.

82 *Ibid.* at para. 2.16. Note that while "business" is defined broadly in s.9 of the *Civil Evidence Act 1995*, "record" is not, so that many computer records will fall instead within s.8.

83 *Ibid.* at para. 3.2.

84 *Ibid.* at para. 2.17.

85 *Ibid.* at para. 3.2.

marks, may be of use in proving that the image has not been altered.[86] In practice, where there has been no challenge to the authenticity of a record, courts may not require extensive proof, beyond oral evidence from an operator of the computer system, that the computer in question was thought to be working properly at all relevant times.[87]

Discussion of the best evidence principle in the context of digital images has led to the proposal of a modified rule in the Select Committee Report. Rather than requiring the production of a paper original of an image submitted as evidence, the new rule would necessitate that any modified copy of an image be accompanied by its unaltered version. Some of the dangers associated with this approach are recognized, however, including the potential for non-disclosure of image alterations.[88]

The Select Committee Report rejects the idea that existing legislation should be modified or supplemented by provisions specifying new criteria which must be met before evidence generated by new technologies, such as digital images, can be admitted. This stance has been taken primarily because further technological change is inevitable, and the law could not possibly keep pace so as not to become outdated in a short period of time. Additionally, such rules could lead to the rejection of evidence, the trustworthiness of which is unchallenged, simply because the proper criteria for admissibility are not met. Ultimately, the preferred approach is to bestow greater power upon judges to decide upon the trustworthiness of computer-generated evidence, taking all supporting evidence into account.[89]

D. Trading Partner Agreements

Opinions vary whether there should be recognition of "trading partner agreements," by which users of electronic records agree between themselves to make use of certain standards for the production, use and exchange of records. These agreements may state that the records as used between the parties are to be admissible in court, but it is arguable that such agreements are attempts to contract out of the rules of evidence.[90] Thus far the proposed Canadian legislation does not express a position on the matter of private agreements relating to electronic evidence arising from transactions between the parties.

E. Authentication Technologies

---

[86] *Ibid.* at paras. 3.2–3.3, 3.21.

[87] *Ibid.* at paras. 3.4–3.5.

[88] *Ibid.* at paras. 3.10–3.13.

[89] *Ibid.* at paras. 3.13–3.19.

[90] ULCC *Consultation Paper*, *supra* note 28 at paras. 74–76.

Authentication technologies such as digital signatures, watermarks and data encryption techniques are seen as possible ways to guarantee the integrity of data, to serve as irrefutable evidence that a particular person is the creator of a particular record or message, and to ensure that data transmitted remains confidential. In addition, these mechanisms may be used as foundation evidence to prove the integrity of a record, as proof, for example, that the record has not been altered since its creation.[91]

A watermark, typically an identifying code or logo, must normally be added to an image at the time it is captured, by a digital camera, for example. While a watermark added to a conventional (non-digital) image will necessarily be visible within the image, a watermark may be embedded within the data of a digital image through encryption, so that it is not possible to view the watermark without the necessary decryption key. Invisible watermarks may be permanent, remaining with the image regardless of whether it is copied or altered, or they may be fragile, so that they will be destroyed by any attempted modification of the image to which they attach. The former would be useful for monitoring copyright violations, for instance, while the latter could provide evidence as to whether or not an image has undergone any changes since its capture.

Alternatively, an entire image may be encrypted and visible only to someone with the proper decryption tools. The use of a digital signature would be one way of achieving this. Typically, a person (the "sender") will create a unique digital signature by using a private encryption key, unique to that person, combined with a "hash function," an algorithm that has been derived from data within the message, image or other document to be signed. This digital signature may be embedded within the document, or it may accompany the document, and the message itself may or may not be encrypted. The digital signature may then be verified through the use of a public key which is related mathematically to the sender's private key. The public key can enable confirmation that the sender's private key was utilized in creating the digital signature, and through computation of the hash function it can be determined whether or not the message was altered since it was digitally signed.[92]

The *PIPEDA* contains numerous provisions which allow, and even require, secure digital signatures to be used as proof of the integrity of electronic documents. Under s.48, technologies or processes which make use of electronic signatures may be prescribed for the purpose of defining "secure electronic signature" within the Bill. This is provided that the technology or process in question produces an electronic signature which is unique to the person using it, the

---

91 *Ibid.* at para. 73.

92 Detailed information on digital signatures can be found within the Digital Signature Guidelines, published by the American Bar Association, Available Online: The American Bar Association <http://www.abanet.org/scitech/ec/isc/dsg.html>; see also Kurzban, *supra* note 25 at 456–459.

technology or process is under the sole control of the person to whom that signature belongs, the technology or process can be used to identify the person to whom a unique signature belongs, and the technology or process can be used to determine whether a document to which the signature has been attached has been altered since it was signed. In the specific context of proposed rules of evidence relating to electronic records, s.56 of the *PIPEDA* (proposed *CEA* s.31.4) states that evidentiary presumptions which satisfy the best evidence rule may be established by regulation, with respect to documents which are signed with secure electronic signatures, as defined within the Bill.

VIII. Planning for Admissibility

Clearly, the law relating to digital image admissibility is far from settled, and it is certain to undergo significant development before long, as the realization is made that existing principles designed for dealing with paper records are not always compatible with emerging technologies. Nonetheless, there seem to be concrete steps which can be taken and practices which can be adopted by users of digital image technologies and records managers, in order to increase the likelihood that a particular digital image will be admissible if submitted as evidence in court. These steps are geared toward proving that an image can be relied upon as an accurate representation of the object or scene which it is claimed to portray, and that the integrity of the image has not been compromised since the image was generated. The primary goal "is to anticipate, and therefore, to be able to negative or explain allegations of distortion."[93]

If possible, the photographer or another witness who has actually observed the scene which is depicted within the digital image should be available and prepared to testify to the accuracy of the image. It is perhaps unwise to place inordinate value upon the testimony of a witness alone when image manipulation is so easily accomplished. However, courts will probably prefer this as the strongest evidence in support of authenticity, in light of the authentication standards traditionally applied to conventional photographs.

It would be helpful if details were made available respecting the system used to produce the digital image. Evidence about the procedures used in the entry, storage, processing and reproduction of data, in addition to proof that the computer system was working properly at all relevant times, could help to establish the integrity of the record-keeping system, from which the integrity of the image itself could be inferred. Also useful would be evidence of any security precautions taken against potential manipulation of records, whether any recognized standards were followed in keeping the records, and whether a business or enterprise regularly or consistently acted or relied upon its records. Though diffi-

---

[93] Fraser, *supra* note 12 at 30.

cult for records-keepers to maintain, an audit trail which shows exactly what happened to a digital image from the time it was recorded would be of great assistance in showing that the record's integrity has been maintained. One possible difficulty to be flagged here is that a person intent on committing fraud would not be inclined to maintain an accurate audit trail.

Authentication technologies such as digital signatures, watermarks and encryption techniques could be employed as security measures against image alteration. If utilized properly, these mechanisms could provide virtually incontrovertible proof of whether or not an image is worthy of trust.

Finally, advance disclosure to an opponent and possibly to the court of a party's intent to use a digital image as evidence could alleviate fears of manipulation, and would allow evidentiary concerns to be investigated and satisfied before trial.

Admittedly, it is unlikely that challenges to admissibility which are so vociferous as to require extensive foundational evidence will arise frequently. Nonetheless, it is advisable that users of digital image technology be aware of the evidentiary concerns that exist, and that some minimal measures be taken to facilitate the making of a reasonable argument in favour of image admissibility, should the situation arise where such support is required.

IX. CONCLUSION

THE FOREGOING DISCUSSION RESPECTING digital image admissibility has given a brief overview of the nature and qualities of digital images which make the application of existing rules of admissibility to this new medium somewhat problematic. The admissibility rules normally applied to conventional photographs and to other forms of computer-generated evidence were examined and related to digital images, within a framework of authentication, hearsay and best evidence considerations. A glimpse was provided of the approaches to digital image admissibility which may be taken in three different countries, and the way in which existing or reformulated evidentiary rules may be used to surmount the concerns which were identified. Finally, a summary was set out of ways in which users of digital image technology can increase the likelihood of image admissibility, should they be adduced as evidence before a court.

A brief examination of the varying approaches to the digital image admissibility problem which are apparently being taken in Canada, the United States and the United Kingdom has revealed that two opposing viewpoints are primarily favoured. In Canada and the United Kingdom, it seems that the dominating preference is to allow this evidence to be easily admitted once a foundation is established which meets a relatively low standard, perhaps simply providing support that the evidence adduced is that which its proponent says it is. Once the evidence is admitted, greater discretion is given to the judge as to the weight it is to be accorded. The evidence is open to attacks from opponents on

its integrity and trustworthiness, and it is up to proponents to defend against those attacks, or to bolster the evidence through further proof of its authenticity, through any or all of the means already discussed. This approach seems preferable to the position taken by many scholars in the United States, who seem to favour a stricter approach which requires substantial foundational or supporting evidence to be adduced before computer-generated records will be admitted. In applying existing rules of evidence to new forms of evidence which have characteristics that are somewhat different than those of paper documents, this perspective seems unduly harsh and restrictive. It is arguable that it is better to facilitate rather than obstruct the admission of all forms of relevant and probative evidence, including computer-generated evidence, and where this requires the introduction of new evidentiary rules then that is a step which ought to be considered.

As a number of commentators have reiterated, the current rules of evidence relating to admissibility have been designed with paper documents in mind, and new forms of evidence which have become prevalent as a result of technological developments often do not easily fit within the existing scheme. It is necessary to get away from rigid traditional conceptions of demonstrative and documentary evidence, and to focus on more practical means of assuring the integrity and trustworthiness of the evidence that is submitted, according to whatever form it takes. It may be desirable for new legislated rules to be established which are specifically directed at standards of admissibility for computer-generated records of various types, including digital images, especially in order to keep the development of the law in this area confined to desirable paths. At the same time, it is important not to adopt an approach which is too restrictive or closely tied to technology that will be subject to significant development, but to employ standards which are adaptable and accommodative to continuing technological advances.