Banking & Finance Law Review
June, 2002

Article

*277 Canadian **Electronic Commerce** Legislation

John D. **Gregory** [FNa1]

Canada has joined the world-wide trend of passing legislation to remove statutory barriers to the legally effective use of electronic communications. The United Nations Model Law on Electronic Commerce has inspired the principal Canadian vehicle, the Uniform Electronic Commerce Act. *The* UECA *bars discrimination against electronic documents, subject to the willingness of parties to such communications to deal electronically. This article discusses the principles and practices of the* UECA, *notably the electronic functional equivalents to writing, signatures, originals and copies, as well as the provincial legislation to implement the* UECA *and the federal and Quebec statutes in the same vein. It also discusses recent initiatives on consumer protection in electronic commerce. Some comparison is made to United States and European parallels. Many Canadian jurisdictions have also passed the* Uniform Electronic Evidence Act *to deal with the admission of electronic records into courts and administrative tribunals. The article outlines the reason for this statute and how it works.*

Canada has not stood aside from the computerization of the world in the past generation or from the more recent move to global electronic ***278** commerce. Nor have we been immune from the legal concerns created by these developments. Our legal system has shared some of the initiatives familiar in the United Nations and elsewhere, while in other respects it has gone its own way. This article will provide an overview of the main thinking in the field in recent years and how it has been reflected in legislation at the federal, provincial and territorial levels.

This article uses the term “electronic commerce” in a broad sense, to extend to the use of electronic communications generally to affect legal relationships. However, much of the discussion here will focus on commercial law in particular, and on the admissibility of electronic records as evidence.

1. PERMITTING ELECTRONIC TRANSACTIONS

(a) The General Law

The earliest legal concerns about electronic transactions have generally arisen from form requirements, or what could be called “medium” requirements, i.e., (apparent) requirements that a particular medium of communication be used for legal effect. The law often demands or presumes the presence of paper. What happens when one takes the paper away?

It is important to appreciate the border between legal requirements and prudent business practice. Many transactions are conducted with paper documents not because the law makes people do it that way but because people are accustomed to doing it that way, or because it makes sense to do it that way, or because it's easier to prove that way. The letter X in pencil on a document is capable in law of constituting a signature. Nevertheless,

most people would not accept a cheque signed only with an X. Likewise, oral contracts are often enforceable as a matter of law, but for high-value transactions, especially with strangers, most people want to "get it in writing."

Where a medium is chosen for prudence and not for legal reasons, the parties are generally free to choose an electronic medium instead of paper. The concern at that point is to judge the reliability of the electronic documents (as well as their provability). [FN1] Most of us do this with less ***279** confidence than with paper documents, since we draw on centuries of experience in knowing what should or should not be done with writing on paper. There is a limit to how much the law can help settle questions of trustworthy practice, and a limit to how much the law should try to do so. [FN2]

The courts can handle some of the legal challenges on their own, as well. In *Rudder v. Microsoft Corp.*, [FN3] the Ontario Superior Court upheld a click-through contract choosing to submit disputes to Washington state courts (as have several American courts). [FN4] A more venturesome case, *Newbridge Networks Corp., Re*, [FN5] held that a corporation could send notice of a special meeting to some of the shareholders by electronic mail, although both the governing statute and the by-laws of the corporation were silent on the point.

That being said, there are numerous legal rules in Canada that appear to require a document on paper. These are generally statutes or regulations, not rules of common law. [FN6] It is, however, important to read legislation carefully. Some legislative requirements that have always been satisfied with paper may not in fact require paper. For example, the *Hotel Registration of Guests Act* [FN7] says that people who run hotels must keep a register of people who stay at the hotel. Nothing in the nature of a register makes it necessary to keep it on paper. Electronic registers meet the existing requirement, without legislative amendment.

***280** Some statutes clearly require paper. Many provinces have a Statute of Frauds that makes some kinds of transaction unenforceable without a memorandum in writing. Ontario's is typical, in some ways. [FN8] British Columbia repealed its Statute of Frauds in 1958, Manitoba more recently. Parallel provisions sometimes appear in provincial Sale of Goods statutes, which are generally based on the *English Sale of Goods Act of 1893*. [FN9] Consumer protection legislation also tends to require executory contracts to be in writing. [FN10] These provisions can be barriers to appropriate use of electronic documents.

An argument can be made that electronic documents are "in writing." Their display involves characters that we commonly consider writing. Each jurisdiction in Canada has a statute for interpreting other statutes, usually called an *Interpretation Act*. [FN11] However, their language varies and often suggests, by example, that writing requires a tangible medium, even if not ink on paper. Ontario's statute says that "writing" includes "words printed, painted, engraved, lithographed, photographed, or represented or reproduced by any other mode in a visible form." [FN12] The more widely held view is that electronic documents do not fall within the statutory definitions, or at least that uncertainty on this point makes a legislative clarification advisable in any event. [FN13]

Statutes for more particular purposes also demand writing or signature or original documents, or use other language that suggests the use of paper, such as "prescribed form" or "certified" or "under hand and seal" or "publicly displayed." The federal government did a study of federal statutes, looking for words and phrases that might force the use of paper, and found a large number. [FN14] The word "writing" appears ***281** over 3000 times in Ontario statutes and regulations; the words "signed" and "original" each over 1500. [FN15]

Over time the various jurisdictions (a compendious term to encompass the federal, provincial and territorial governments) have enacted statutes and made regulations to resolve particular problems, or to permit particular

uses of electronic documents. Ontario repealed writing requirements applicable to general sales contracts in 1994. [FN16] Ontario also passed the *Electronic Registration Act (Ministry of Consumer and Business Service Statutes), 1991*, [FN17] under which filings under the *Personal Property Security Act* [FN18] have been done electronically for several years. Land registration is beginning to be done electronically in Ontario, using digital signatures, with the authority of legislation passed in 1994. [FN19] Ontario also adopted a statute allowing the Minister to prescribe forms for doing electronically the business that many statutes require to be done with the government. [FN20] Nova Scotia and Newfoundland have similar statutes. [FN21] In 1998, British Columbia passed a statute to facilitate electronic filing of information with the provincial government [FN22] and Saskatchewan did likewise. [FN23] Many more examples could be given. [FN24]

Such piecemeal and local initiatives are widely recognized to be inadequate to resolve the concerns among business people, governments and the general public about the state of the law applicable to electronic communications. On the contrary, solving individual problems with narrowly focused statutes, or with judgments in individual cases on ***282** specific facts, risks creating a patchwork of inconsistent legal rules that will make electronic communications harder rather than easier, even within a single jurisdiction. We turn now to more widely applicable measures to remove statutory barriers to electronic transactions and to promote their use where appropriate.

(b) Uniform Electronic Commerce Act (UECA)

The international standard for removing statutory barriers to electronic commerce is the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, recommended by the General Assembly for adoption in all member countries of the United Nations in 1996. [FN25] Many countries have enacted laws based on the *U. N. Model Law*, including Australia, Ireland and Singapore. [FN26] The American uniform statute based on that model, the *Uniform Electronic Transactions Act* (*UETA*), was adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in July, 1999. [FN27]

Canada participated in the preparation of the *U. N. Model Law* and has taken steps to implement it. Consistency with the laws of our principal trading partners on electronic matters was thought important, especially in an increasingly borderless electronic trading environment. To put the *U. N. Model Law* into Canadian statutory language, the ***283** Uniform Law Conference of Canada adopted the *Uniform Electronic Commerce Act* (*UECA*) as of September 30, 1999, and recommended it for adoption by the member jurisdictions of the Conference - all the provinces and territories of Canada and the federal government. [FN28] Notes on its implementation across the country appear below, after the discussion of the UECA itself. [FN29]

The *Uniform Act* can be considered a minimalist response to the quest for certainty about the legal status of electronic communications and electronic records. It is minimalist for several reasons. First, the existing law - statutes and common law and private law based on contracts - is capable of resolving a good number of questions on its own. Electronic messages, even on the Internet, do not present radically new questions in every field. Next, the technology underlying electronic records is changing rapidly, so attempts to prescribe specifically how to conduct legally effective communications risk obsolescence even before they come into force. In any event the uses to which electronic communications are put vary so widely that no single technology would suit all of them. The statute can be said to be “technology neutral” for this reason. Finally, e-commerce is global in scope, and we do not want to take a seriously different approach from our major partners. The international consensus today is arguably in favour of minimalism, as shown by the Model Law itself and the number of countries implementing it.

(i) Scope

The *Uniform Electronic Commerce Act* applies not only to commercial transactions, as its name might suggest, but to all rules of law that are not excluded from it. That makes the list of exclusions important. Most of the list is itself a matter of international consensus, in that several of the laws that purport to enact the *U. N. Model Law* have similar exclusions. The Model Law contemplated that enacting countries would exclude some laws from its rules but did not specify any itself. [FN30] Wills and testamentary trusts and dealings in land are common exclusions. ***284** The *UECA* does apply to transfers of land that would not require registration to be enforceable against third parties. [FN31] This allows for electronic short-term leases, for example. In the U.S., land transfers are not excluded, but an electronic transfer would not be good against third parties unless registered, and particular registration systems may not accept electronic registration. [FN32] The Canadian view was that allowing for the creation of electronic transfers good only between the parties might expose less sophisticated parties to undue risk. [FN33]

The *UECA* excludes negotiable instruments and negotiable documents of title. [FN34] The American *UETA* does not exclude negotiable instruments as such - section 16 deals in detail with “transferable records” - but many of the main provisions of the Uniform Commercial Code touching such documents are excluded. [FN35] A New Brunswick consultation paper on electronic transactions legislation [FN36] suggested that negotiable instruments should not be excluded. The reason for their exclusion is that such instruments need to be unique, because the instrument itself has value as it is negotiated. It is not yet possible to create an uncopiable electronic document without immobilizing it, which negates the precondition of negotiability, namely transferability. New Brunswick says that if no electronic negotiable instruments can exist, then it is not necessary to exclude them. If technology and the market work out a method of ***285** creating and using such instruments, then the law should let them do it. [FN37]

The Canadian *Uniform Act* also excludes powers of attorney for personal care (which may take the form of advance health care directives) and for the financial affairs of an individual. As with the land transfers mentioned above, and wills, the concern with these kinds of documents was that they are often created by unsophisticated people, often without legal or technical advice. It was thought that there was too much risk of undetectable fraud or loss of integrity of data unless more specific security measures were provided, more than a uniform and fairly generic statute could give. New Brunswick suggests that they are just examples of agency contracts, which are not generally excluded. [FN38]

There is no implication that any document excluded from the *Uniform Act* should never be created electronically. [FN39] Ontario has a detailed scheme for electronic land transfers and registration, for example, but it rests on a particular set of statutory and regulatory rules to ensure that it works properly. [FN40] Other provinces are working on electronic land registration as well. [FN41] The Uniform Law Conference of Canada considered legislation on electronic wills in 2001, but decided to make only limited provision for them in its statute. [FN42]

The scope section also provides that the *Uniform Act* yields to any other statute that expressly regulates, permits or prohibits the use of electronic communication. [FN43] The Conference thought it inappropriate to override legislated standards, even if the standards are out of date or ***286** inadequate. The point of the Model Law is to remove barriers, not to reform the law where the barriers have already been addressed. However, the Act provides that using words like “in writing” or “signed” does not constitute a prohibition against using electronic communications, since otherwise this exclusion would undermine the operation of the Act itself. [FN44]

One purpose of the *Uniform Act* is to permit the use of electronic documents without individually amending all the statutes that could bar their use in some way. In case a government learns after enacting the Act that some

unnoticed statutory provision or class of document should not be subject to the general permission, the Act allows the addition of exclusions by regulation. [FN45] The New Brunswick consultation paper suggested that all exclusions should be made by regulation, so that they can be removed or adjusted as technology and market practices evolve. [FN46]

(ii) Consent

The basic principle of the *UECA* is that information must not be denied legal effect merely because it is in electronic form. [FN47] Particular requirements as to form are dealt with in specific provisions later, and the general principle does not override the specific rules. That said, it is crucial to note that the *UECA* does not require anyone to use or accept electronic documents. The rule against discrimination does not prevent any person from refusing to accept electronic documents; the rule essentially applies in determining legal rights as between consenting parties. The Guide to Enactment of the *U. N. Model Law on Electronic Commerce* says that the Model Law is not intended to compel the use ***287** of data messages, [FN48] but the text of the Model Law itself is silent on the point. The *UECA* sets this out expressly. [FN49] The *UETA* has a similar provision, drafted in even stronger terms, since it requires an agreement, not just a unilateral consent, and the statute does not even apply in the absence of such an agreement. [FN50] The *Australian Electronic Transactions Act* also looks for consent, on a rule-by-rule basis. [FN51] As a result of the consent provisions, the fact that an electronic document complies with the rules for satisfying form requirements, discussed in more detail below, does not make that document binding on someone who does not want to deal electronically at all. More accurately, compliance with the *UECA* (i.e., its implementing statute) does not itself make the electronic document binding. The Act is neutral on the point. People may bind themselves by contract to accept electronic documents, and other law - including, for example, employment law - may compel them to do so.

The *Uniform Act* is intended to remove barriers where people want to use this technology. Since most electronic communications, and certainly most commercial transactions, will be on consent, this will not usually be a problem. Consent to use electronic documents may be inferred from conduct, moreover; an express agreement is not needed. Otherwise there is too much risk of bad faith refusal. Questions arise about how much consent is needed and how broad it may be. If one puts an e-mail address on a business card, has one consented to deal electronically for all purposes? The probable answer is that it would be a presumptive consent for the purposes of the business related to the card, but not otherwise. Someone who wanted to be sure to make a binding ***288** deal electronically would want to make more sure of the consent. An exchange of electronic messages in view of a deal would surely constitute such a consent. However, failing to protest an e-mail message is unlikely to be taken as consent to receive its content electronically, without a pattern of dealing in that medium.

The need for consent can cause some risks in using electronic documents that need to be good against the world, or against people unknown when they are made, such as some powers of attorney. Business users of such documents are likely to develop a practice of accepting them, no doubt subject to conditions as to their reliability, and such a practice could be taken as consent to accept the next one they get as well.

The consent rule is absolutely fundamental in a technology-neutral statute, i.e., one that does not prescribe the technology to be used to create legal effects. The proposed user of electronic communications can decide if the technology to be used for the communications is sufficiently reliable for his or her purposes. Only the proposed user can make that judgment for his or her own purposes. The power to say No is the power to say Yes, if ... the system is secure enough, or satisfies other concerns of the recipient. [FN52] It is also important to note that the consent is not necessarily comprehensive. One may accept some kinds of information in electronic form and reject others, or accept it for some purposes, or accept electronic documents but not electronic

signatures. The consent rule does not undermine the general principle of the *UECA* that the law should not discriminate against information in electronic form, but it sets an important limit on that principle. [FN53] The consent to deal using electronic documents also must not be confused with the presence or withholding of consent to participate in any particular transaction,***289** so that, for example, consent to the medium is not in itself acceptance of an offer of a contract.

(iii) Functional Equivalents

Many rules of law use language that requires, or appears to require, the use of documents on paper. When the *UECA* says "a requirement under [enacting jurisdiction] law," [FN54] it covers not just statutes and regulations but any other source of law. As with the *U. N. Model Law*, it covers rules that provide consequences for the absence of paper, as well as direct commands. [FN55] Following the *Australian Act*, [FN56] it also applies to "permissions" to use electronic documents, e.g., where the use of a particular process is given a particular legal effect (e.g., "A document signed by a public official is admissible in evidence"). [FN57]

The Model Law and the *Uniform Act* expand these rules to cover documents in electronic form. They do so by creating "functional equivalents" to the paper documents. [FN58] In other words, they do not simply define writing as including an electronic record, or define signature as including an electronic signature. This was thought too rigid an approach that risked including too many electronic records or allowing electronics in too many situations. Rather, the law seeks to isolate the essential policy functions of the requirement and state how those functions can be achieved electronically. The basic form of the rule in the Act is ***290** therefore "where the law requires [paper], that requirement may be satisfied by an electronic record if [certain standards are met]." The standards themselves vary but are stated in general terms.

The principal effect of this approach is to turn questions of capacity ("Am I allowed to do this electronically?") into questions of proof ("Have I met the standard?"). Since meeting the standard is often a matter of agreement between the parties to a transaction, this seems a useful contribution. As noted earlier, meeting the standard gets one past the form requirement. It does not mean that the electronic information is effective against a person who does not want to deal electronically. The electronic information would also have to meet other requirements that the law imposes on any information intended for its purpose. Contracts still need consideration, financial details may still have to be disclosed, and so forth.

(A) Writing

The basic function of writing is memory. The *UECA* therefore says that a writing requirement can be satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference. [FN59] This formulation rests on a fundamental principle of the *UECA*: the electronic system does not have to be better than the paper system it replaces. [FN60] Just as a paper document may last a long time or be destroyed quickly, so too the *UECA* does not say how long the electronic information has to be usable. If, however, there are other rules about the length of storage, for example in a record retention rule, then the electronic information would have to satisfy that rule too. That is dealt with expressly in the *UECA*. [FN61] "Accessible" means understandable as well as available. However, an electronic document may be accessible and usable***291** if it can be treated appropriately by a machine; the document does not have to be in a form readable by a human being to meet the test. [FN62]

It will be noted that the *Uniform Act* and the statutes that implement it [FN63] are drafted to distinguish between documents in writing and documents in electronic form. In other words, they implicitly reject arguments that the word "writing" includes electronic information. It is hard to read the new legislation as including electronic documents as "writing," and treating the standards in the Act only as additional guidance on how to deal with this particular aspect of writing. It is fair to say that the drafters of the *Uniform Act* did not

have this reading in mind. [FN64]

In the United States, the *UETA* deals with the policy function of writing, as discerned in the Model Law, through the use of the term “record.” [FN65] This term was adopted by *NCCUSL* some years ago as a media-neutral term for some kinds of information. It is defined as “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” [FN66] The last quality is what ties it to the Model Law: “retrievable” and “perceivable” serve the same function as “accessible” and “usable.” The American formula does not set a standard for durability either. [FN67] Moreover, the duty to make an electronic document accessible does not require a person to provide computers to any potential reader of the document, any more than the person must make a copy of a paper document for anyone who asks, just because the document must be in writing. If the existence of the document in writing is an issue, then that will have to be proved to a court, just as a court would have to be shown the document on paper. If a person who must be able to have access to the document does not have a computer, then it will be difficult to conclude that the person consents to receive the document in electronic form.

***292** The *UECA* speaks frequently of “electronic documents,” a term that is not defined, though “electronic” is given an expansive meaning to cover existing and future technologies that may not be technically electronic. [FN68] The definition would extend to electronic recordings of speech, such as a voice mail message or a record created by a computer through voice recognition. The Australian statute excludes orally-generated electronic messages unless they produce a record reproducible as writing. [FN69] The Uniform Law Conference decided after discussion not to exclude electronic records of oral communication. The Conference did not want to restrict the development of technology, and in times of converging message systems, the person who sends a message in one medium may not know the medium in which it will be received. The legal consequence of messages should not depend on unpredictable factors, such as whether the recipients have their telephone forwarded to a pager, or their e-mail forwarded to a voice mail system.

The *UECA* deals with two other aspects of writing. If information has to be delivered, and not just be in writing, then section 8 requires that the information in electronic form must be capable of being retained by the addressee. [FN70] Just as I cannot deliver a paper document to you by ***293** simply showing it to you, I cannot deliver an electronic document by putting it on a web site. [FN71] The addressee must be able to decide how long to keep the information, without risk that the person providing it will alter or delete it. The principle of this provision came out of the Uniform Law Conference of Canada; the current language originated with *NCCUSL*. [FN72] The original draft language required that the addressee be given control of the electronic document, again as a protection against its alteration by the originator. [FN73]

Sometimes the law requires information to be provided in a particular form. An electronic document can satisfy this requirement if the information is laid out in substantially the same form. [FN74] It is not the intention here to prevent the use of formatting codes, such as are common in electronic data interchange systems. Information can be transmitted as economically as possible by electronic means. However, the practical display of the information should be recognizable as being the form required by law. [FN75]

If the law requires a form of display or communication, then the electronic document has to satisfy that. [FN76] For example, the capacity of a public place may have to be posted conspicuously in that place. The landlord's address may have to be displayed in the entry to a rental building. Information may have to be delivered by registered mail. While information in electronic form can meet these requirements - for example***294** one could deliver a diskette by registered mail - the Act does not allow people to avoid them by using electronic documents. This provision was directly inspired by *UETA*. [FN77]

The New Brunswick paper mentioned earlier [FN78] suggested that the general provision was unnecessary, since the non-discrimination clause (section 5 of the *UECA*) says that information is not invalid solely by reason that it is in electronic form. Failure to comply with other requirements would not be remedied by section 5, if the word "solely" were taken seriously. [FN79] This illustrates a tension that arises in drafting even minimalist statutes, between saying the very minimum possible and spelling out some of the consequences of the basic rules, even if the consequences might be understood from the basic rules themselves. Some of the differences in drafting between the *UECA* in Canada and the *UETA* in the United States arise from different answers to this kind of question. [FN80]

(B) Signatures

In all its functional equivalence rules, the *Uniform Act* does not intend to change the substance of the existing law. It intends only to make the law media neutral, equally applicable to paper and to electronic documents. The treatment of "electronic signature" therefore does not create a new legal "thing" with this name. Rather it deals with the essential functions of any signature. The definition reads, "'Electronic signature' means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document." [FN81] The legal essence of a signature is the intention with which it was made, rather than its form or medium. The definition says that the electronic information must be made or adopted "in order to sign a document." The use of the word "sign" was deliberate, ***295** and is found in the *UETA* as well. [FN82] The existing law about the appropriate intention for an effective signature, and how one proves it, continues in effect. [FN83]

The purpose of defining electronic signature is to make clear that the electronic version does not have to look like a handwritten signature when it is displayed. It may be code or sound or symbol of any kind, if the intention is present. [FN84] Likewise, a signature may travel apart from the document it signs, if the association with the document is clear. The signature may be in the document but also may not be. Also, the wording of the definition would allow one to contemplate an electronic signature used to sign a document on paper, if the connection between them were clear.

The *UECA* provides that a signature requirement can be met by an electronic signature. [FN85] Unlike the *U. N. Model Law*, [FN86] it does not go on to require that the electronic signature must be as reliable as is appropriate in the circumstances. The Canadian statute agrees with the *UETA* in this regard. [FN87] At common law, and arguably in the Civil Law of Quebec as well, a method of signature on paper does not have to meet any test of reliability. If the association with a person is demonstrated and the intent to sign is demonstrated, the signature will meet the signature ***296** requirement. [FN88] Those elements will have to be shown in order to meet the definition of electronic signature. As noted earlier, the *Uniform Act* is not trying to make the law better, just neutral.

The intent of a signature and its legal effect can never be determined simply from the form of the signature, whether on paper or in electronic form. The context is always needed, even if it is as little as the words "I agree" accompanying the signature. [FN89] A signature without context is simply an autograph. The signature permits the identification of the signer, [FN90] possibly along with other evidence of identity. [FN91] In other words, a signature is mainly evidence of attribution - to link a person with a text. Other evidence of attribution may be enough to rely on without the signature. The rest of the document shows the legal effect to be given to the document signed by the identified person. The content of the document, and thus context for the signature, is more important than the physical characteristics of the signature itself.

***297** However, it is possible that the authority that imposed the signature requirement in the first place did have some degree of reliability in mind. In that case, the *UECA* allows that authority to make a regulation

imposing the reliability standards of the *U. N. Model Law*. [FN92] Meanwhile, *UNCITRAL* has created a new Model Law on Electronic Signatures, one of the main purposes of which is to help the parties determine in advance whether the reliability standard has been met. [FN93] The *UECA* and even the *U. N. Model Law on Electronic Signatures* avoid detailed descriptions of the technology to be used, however. The uses of signatures are too varied for any one method to suit them all. In any event, technology is evolving too quickly to fix any particular version of it in law. Either the law would be irrelevant or it would impair innovation by channeling concepts in a particular direction. A broad use of electronic communications would not be served by such a statute.

This discussion will remind the reader of another key principle of the *Uniform Act*, mentioned earlier: there is a distinction between basic legal requirements and prudent business practices. A name typed on the bottom of an e-mail may be a valid signature, but it may not be trustworthy enough for many people to want to rely on it in practice. What people want in practice will depend on many factors, including the context, the course of dealings of the parties, the use to which the signed document is to be put, and so on. The elements of reliability of attribution of a document are many, and the technical aspects of the signature, on paper or electronic, are only a part of the "threat/risk analysis." We have ***298** seen earlier the role of the consent rule [FN94] in giving people the power to insist on such considerations.

Article 13 of the *U. N. Model Law on Electronic Commerce* provides that data messages may be attributed to those who create them or who authorize their creation. This, of course, is the general law in Canada and the United States. The *UETA* [FN95] and the Australian statute [FN96] have similar provisions. The Canadian Conference thought this went without saying, so did not say it. The *U. N. Model Law* goes on to provide a rule [FN97] of attribution where certain agreed security procedures are used on data messages. *NCCUSL* attempted to devise similar rules, but they fell under severe criticism based partly on the fluidity of the technology available and partly on the likely lack of sophistication of its users. [FN98] The Canadian Conference did not try to follow the Model Law on this point in the *Uniform Act*, but the federal government has given it some echo in its legislation, discussed below. [FN99] Some of the recent work of *UNCITRAL* on electronic signatures aimed to give more substance to the provisions of Article 13, but there too, efforts to draft clear attribution rules ended up much narrower than originally hoped. [FN100]

As a result of the silence of the *UECA*, parties to electronic transactions will have to satisfy themselves of the origin of electronic documents and signatures. What is prudent will depend on the circumstances, including the other identification methods available (such as use of a credit card), the total value of the transaction and the cost of getting better assurance of origin. A technology-neutral statute can do little more ***299** without hampering parties who are capable of making their own decisions.

(C) Originals

When the law requires a document in original form, it is seeking assurance of the integrity of the document, that it has not been altered. The *UECA* reproduces this function in section 11, following the *U. N. Model Law* in Article 8. [FN101] The notion of "original" is hard to apply to electronic documents, because of the way they are generated. A "copy" is identical in all respects to the "original," so the reasons for wanting an original may be hard to meet from that status alone. The rule in section 11 would apply whether the document was first created on paper and later became electronic, say by scanning or faxing to an e-mail system, or whether it was in electronic form at all times. [FN102] The organization of the information must be reliably similar to that in the original too. The format of information is part of the information itself. The *UETA* has a similar provision, though it mixes original requirements and record retention rules. [FN103]

(D) Copies

Copying electronic documents can be very easy. However, it is harder to understand how to comply electronically with a requirement to furnish a number of copies of a document. First, it is very difficult, as noted above, to distinguish between an original and a copy. Next, there are a number of ways in which one could provide, say, three copies: send the same e-mail three times, attach the same text three times to one e-mail, put three versions of the document onto a single diskette, remit three diskettes with one version of the document on each, and so on. To avoid this rather sterile discussion, the *UECA* provides that only a single version of the electronic document needs to be furnished to a single ***300** address, where the law requires copies. [FN104] The recipient can decide how best to make the additional documents. This provision has no parallel in the United States or the European Union, but Quebec has incorporated it into its legislation on the subject. [FN105]

(iv) Government Documents

The *Uniform Act* contains a number of special provisions about documents sent to government. The concern it addresses is that governments receive a lot of information from a lot of people, many of whom are communicating involuntarily and with many of whom the government has no contract by which the methods of communication could be agreed. To protect the government from an overwhelming variety of formats and hardware, therefore, the provisions on consent require express consent by government, rather than implied consent. [FN106] Moreover, the rules on providing information, on forms, on signatures, and on originals say that governments may impose their own technical requirements for satisfying these sections. [FN107] Documents originating with government, however, would have to meet the general standards of the Act. [FN108]

A very similar structure is found in the Australian Electronic Transactions Act. [FN109] The *UETA* also has special provisions on government documents. [FN110] The Canadian federal Act requires a central register of designations and regulations for the use of electronic documents under federal law, [FN111] which allows the government to protect itself case-by-case as it sees fit. The *UECA* has no set requirement for communicating government choices, except that consent must be notified to people likely ***301** to be affected by it. [FN112] The *UETA* states the merits of interoperability of technology but does not require it. [FN113]

The *UECA* defines “Government” to include core government departments and agencies, but not Crown corporations, which are thought to be more like commercial operations. [FN114] Each enacting jurisdiction will have to decide on the appropriate scope for this definition. Likewise, municipal governments may need the same kind of protection against multiple formats, but it may be thought that the risk of hundreds of inconsistent technical standards from hundreds of municipalities may require a more centralized solution. [FN115] The *UECA* is silent on whether the courts are part of government, [FN116] unlike the Australian [FN117] and American federal statutes, [FN118] which exclude them, and unlike the *UETA*, which includes them. [FN119]

Section 16 of the *UECA* provides for electronic forms, whether or not forms on paper are already prescribed (and whether or not the forms are used to submit information to government or between private parties). Section 17 allows governments to use electronic communications for all their purposes. Section 18 authorizes incoming and outgoing payments to be electronic, if the main financial authority of the government consents.

(v) Contracts

The *UECA* follows the *U. N. Model Law* in providing some basic rules about electronic contracts. [FN120] The volume of electronic commerce conducted under the pre-*UECA* law may suggest that businesses were not much impeded by doubt about the validity of such contracts. Nevertheless,***302** the *UECA* covered a few points in the interests of greater certainty.

The main question about such contracts appears to be whether sending some kinds of electronic signals can

show sufficient intent to be bound by contract. The *UECA* says that an action in electronic form, including touching or clicking on an appropriately designed icon or place on a computer screen, is sufficient to express any matter that is material to the formation or operation of a contract. [FN121] It seems apparent from this that a voice-activated communication would also be effective. [FN122]

Section 21 and 22 provide for the use of electronic agents. Electronic agents are defined as computer programs used to initiate an action or to respond to electronic documents without human intervention at the time of response or action. [FN123] They have nothing to do with the law of agency, since they are machines that have no legal personality. The term is, however, widely accepted and not easily displaced by something clearer in law, such as "electronic device." [FN124] The *UECA* makes it certain that contracts may be formed using electronic agents, on one side or on both sides, [FN125] even if it is hard to attribute conscious intent to contract to a legal entity for the specifics of a contract determined by the (software) agent.

Section 22 provides a solution for the "single keystroke error," where a human being makes a mistake in communicating with an electronic agent. Often such agents are not programmed to recognize messages intended to correct an error, e.g., "I didn't mean 100 widgets, I meant 10." The section makes these mistakes unenforceable where an individual [FN126] follows the procedures set out there, unless the owner of the agent provides a method of preventing or correcting errors. It is not ***303** the role of legislation to say exactly what method must be used, as there may be many acceptable ways. Restating an order before processing it, with a note like "This is what you are ordering. Are you sure?" would probably be enough. This provision was borrowed largely intact from the *UETA*. [FN127] It does not override the usual laws of mistake in contract; [FN128] it adds an additional remedy where electronic agents are involved, because of the novel risk in such transactions.

The *UETA* otherwise has similar rules on contracting. The EU has a Directive on Electronic Commerce that ensures that such contracts are valid, but imposes extra obligations where consumer transactions are involved. [FN129]

(vi) Sending and Receiving Electronic Documents

The *U. N. Model Law* has influenced the *Uniform Act* in determining where and when messages are sent and received. The location question is easier. The basic rule, subject to agreement of the parties, is that messages are sent from and received at the place of business of the sender or recipient. Subsidiary rules deal with multiple places of business or no place of business. [FN130] The rule helps separate the essence of the communication from the incidental aspects, such as the location of the server, or the location of the sender or recipient when he or she actually deals with the message. Thus someone with a business in Toronto who has an e-mail account or a web site with sympatico.ca does not have to worry about where sympatico's server is, [FN131] and does not change the law relating to a transaction by sending or picking up messages on the computer while travelling out of the province. [FN132]

***304** There may be cases where the location of the server or other *indicia* of location remain important, of course, such as in deciding if one has a permanent establishment for tax purposes. [FN133] Jurisdictional questions in electronic commerce are tricky and lend themselves poorly to legislation. The rules in the *Uniform Act* will resolve a few but far from all. [FN134]

The *Uniform Act* then deals with the time of sending and receiving electronic messages. The rule on the time of sending is relatively simple: the message is deemed sent when it leaves the control of the sender. If the sender and the addressee are on the same system, then the message is sent when it becomes accessible to the addressee. [FN135] The purpose of this kind of provision is particularly to dispose of the question of intermediaries such as

communications agents or computer service bureaus; it is the ability of the parties to control and retrieve the messages that counts, not the passage of the message through intermediate machines.

The somewhat more difficult issue is time of receipt. The *U. N. Model Law* deems a message received when it reaches an information system designated by the addressee for receiving electronic messages, or if no system is designated, when it enters an information system of the addressee. [FN136] The *UETA* requires that the addressee have designated or used the system for the purpose of the kind of message in question, before that rule applies. [FN137] The *UECA* adopts the designation or use ***305** point, but makes receipt a presumption not a rule, as it is in the Model Law and the *UETA*. [FN138] It was widely thought among the working group that the receipt of electronic messages is not reliable enough to support a rule that cannot be rebutted. [FN139] Creating a presumption of receipt for messages sent to designated systems essentially creates a duty on the addressee to check the designated system for messages, or at least a risk if the addressee does not check. There is arguably no duty to check undesignated systems; receipt is not presumed until the addressee has actual notice of the message. [FN140]

In the absence of a rule or presumption, or if the presumption is rebutted, the sender will have to demonstrate actual receipt. The *UECA* does not specifically deal with determining the fact of sending and receiving, separately from the time. The working group thought it was too difficult to distinguish these elements separately, and possibly artificial as well. If one can demonstrate the time of sending or receipt, it is hard to imagine a successful challenge to the fact that the message was sent or received. Sometimes the fact may be important and the time unimportant, but the time element determines both, except where the presumption of receipt is rebutted and all facts, including the fact of time, must be proved directly. [FN141] If senders need to be sure of receipt ***306** before taking further steps, they may have to ask for acknowledgements. [FN142]

(vii) Carriage of Goods

One of the last things that *UNCITRAL* added to the *U. N. Model Law* was a section on special transactions, namely those dealing with the carriage of goods. [FN143] It was thought that these are very often international transactions, and they are subject to a number of special legal regimes and conventions. In particular they often rest on negotiable documents of title such as bills of lading. The general principles of the *U. N. Model Law* on non-discrimination based on medium apply here too, but it was thought that particular rules were needed for negotiability and for the possibility that documents would be transferred from one medium to another when the document itself carried legal effect. [FN144]

The *Uniform Act* has picked up these provisions. [FN145] It has not spoken of “unique” documents, however, as it is not clear how to create a unique electronic document (though one can immobilize and time-stamp an electronic document). Instead, the *Uniform Act* speaks of a document intended for one person and no other person. [FN146] Representatives of transport organizations have favoured enacting these provisions, even though it is not clear yet what technology may be able to satisfy the requirements. [FN147] To date few if any other countries have adopted these provisions of the Model Law. As noted earlier, the *UETA* offers provisions on “transferable records,” [FN148] and some early work has been done to give ***307** them legal reality, but not in the transportation field so far. [FN149] The EU has no equivalent yet.

(c) Provincial Legislation on Electronic Documents

All of the provinces and one territory have legislated recently on electronic documents and electronic commerce. [FN150] All but Quebec have followed the Uniform Electronic Commerce Act. [FN151] Only a few of them vary much from the *Uniform Act*, and only two - Manitoba and New Brunswick - in significant principle. This paper discusses the Ontario statute, as it has some interesting variations in wording, if not principle, and also the salient points of the Manitoba and New Brunswick acts. It is important for anyone relying

on the provincial statutes to read them carefully, however, since small changes in wording from the *UECA* may ***308** have a significant impact, even if not apparently intended by the implementing jurisdiction.

Minor variations elsewhere include the following. British Columbia's bill does not contain special rules for government at all, except to permit electronic payments. Saskatchewan has a separate part for electronic communications with government, based on its 1998 e-filing statute referred to in the first section of this paper about electronic transactions. [FN152] Prince Edward Island defines “electronic signature” differently from the other provinces, [FN153] using language like that of the federal statute for “secure electronic signatures,” but without the detailed applications or the regulatory support that the federal government has adopted. [FN154] The narrow language may limit the acceptability of electronic signatures that would have been acceptable with no legislation, [FN155] or under the uniform terminology. Nothing in the legislative history of the PEI statute [FN156] hints at the reasons for the change. [FN157]

(i) Ontario's Legislation

Ontario's Electronic Commerce Act does not vary significantly in principle from the *Uniform Act*, but it is laid out somewhat differently. The definition section includes municipalities as “public bodies,” the term Ontario uses for the *UECA*'s “government.” [FN158] The *Ontario Act* allows the province to designate bodies by regulation as public bodies. [FN159] ***309** The relation to the Crown is sometimes unclear, and the need for the protection of the government document provisions may vary. The regulatory power ensures that the protection can be provided where it appears necessary. Ontario, however, excludes election documents. [FN160] Elections are run with a widespread and informal apparatus, involving makeshift quarters and volunteer labour. It was thought that much more security would be needed for an effective electronic system than was provided for in the *UECA*. While one might argue that election officials could simply wait till they were satisfied with the security before going electronic - the *UECA* would not compel them to use such methods - nevertheless the risks of some of the several hundred municipal systems using electronic voting prematurely seemed worth avoiding. [FN161] In addition, election officials might not want to have to ascertain the consent of each potential voter to using the electronic system, and to have to have available some non-electronic equivalent. The *Electronic Commerce Act* itself does not allow a public official to require the use of electronic processes. [FN162] It might be noted that Ontario currently allows electronic filing of campaign finance reports.

Ontario added conditions to the *UECA*'s implied consent rule, requiring that the person relying on it must have reasonable grounds to believe the consent is genuine and relevant to the communications in question. [FN163] While these additions aim to relieve some concerns of consumer advocates, it is hard to imagine a serious businessperson relying on implied consent without a belief in these matters. [FN164]

Ontario has added a rule on providing information, saying that information that has by law to be provided cannot be provided simply ***310** by giving access to it on a web site. [FN165] There must be a real delivery of the information to the person to whom the provider is required to provide it. However, web-based e-mail delivery is acceptable, as is provision in the course of an interactive web transaction. [FN166] It may be appropriate for particular rules on providing information to be satisfied by putting the information on the web - perhaps with direct notice to the addressee that it is there - but it was felt not to be appropriate to make such a rule across the board.

This has raised an interesting issue for issuers of securities. A National Policy of the Canadian Securities Administrators [FN167] allows public companies to post notices and financial information on their web sites rather than sending them to shareholders, where the shareholders have consented to forego direct delivery. A similar rule is in effect in the United States through the Securities Exchange Commission. [FN168] However, the Policy does not override Ontario's provision. There is an argument that if securities issuers follow the “know

your client" rule as required by securities administrators and take the steps required by the Policy for consent of shareholders, then they have done more than "merely" make information available for access, and thus do meet the requirements of the Act for "providing" information in electronic form. It may be worth noting that if the Policy were converted to a regulation, then it would fall outside the *Electronic Commerce Act* altogether, as a rule of law regulating electronic communications. [FN169]

The *UECA*, followed by Ontario, allows an electronic document to serve as an original if it has sufficient assurances of integrity. It was pointed out at the hearings of the legislative committee [FN170] that this could ***311** lead to confusion in some kinds of financing transactions. The *Personal Property Security Act* [FN171] provides that possession of certain chattel paper, notably documents of title, prevails over registered security interests in the goods represented by the paper. In cases of carelessness or fraud, it was conceivable that a paper original of such a document would coexist with an electronic functional equivalent of an original, purporting to give the same interest in the same collateral. Nothing in the language of the *PPSA* or the *UECA* permitted the resolution of this conflict. In the end, Ontario added a subsection to *the Electronic Commerce Act* [FN172] to ensure that the paper original would prevail. If the *PPSA* is amended to account generally for electronic security documents, [FN173] then different priority rules might be worked out. To date only Nova Scotia has picked up this variant to the *UECA*. [FN174]

Ontario has added a subsection [FN175] to the *UECA*'s provisions on electronic signatures, to allow for regulations spelling out particular signing methods for particular transactions or documents or persons. It has made no regulations as of the date of writing and does not expect to make many regulations in the future, but the power to be specific on occasion was thought valuable. The *Uniform Act*, as noted, provides for regulations stating the reliability test of the *U. N. Model Law* on Electronic Commerce, [FN176] which merely requires that a signature be as reliable as appropriate in the circumstances.

***312** Ontario also added in late stages of passage a provision about electronic seals, on which the *Uniform Act* and the other provincial statutes are silent. Seals are still used in several types of transaction in Canadian law. [FN177] Because of the variety of situations and legal effects, [FN178] the statute itself does not say how to do them, it merely gives the Lieutenant Governor in Council power to make regulations to allow an electronic document to be considered sealed. [FN179] The government may make regulations permitting electronic processes for some functions of seals while leaving the others on paper alone.

Ontario also made it clear that an electronic signature may constitute an endorsement, though an electronic document has no "back." [FN179a] This may be thought to be self-evident, but not everyone interpreting the legislation may want to give it a broad meaning. Compare the Quebec statute: "Similarly, differences [between documents in different media] relating to page numbering, the tangible or intangible nature of pages, format, recto or verso presentation, total or partial accessibility, and sequential or thematic information retrieval possibilities shall not be considered as affecting the integrity of the documents." [FN180]

Ontario has also provided that its statute does not apply to the use of biometric information as a personal identifier, without express consent of the person involved or without legislative authority. Concern was expressed by privacy advocates that the use of such information could facilitate the matching of data across diverse fields, using biometric information as the key. [FN181] The statute does not prohibit the use of biometrics for the stated purposes, but it may not be relied on to give legal ***313** effect to their use unless their use is expressly authorized. The caution was thought helpful because Ontario does not have private-sector privacy legislation that might otherwise protect the same interests. If such legislation were to be passed, as the government has announced, [FN182] Ontario might repeal this provision of the *Electronic Commerce Act*.

The *UECA* does not invalidate other rules of law, though it interprets them to facilitate the use of electronic communications. Nevertheless, for greater certainty the *Ontario Act* provides expressly that it does not override freedom of information or privacy laws. [FN183] It also makes clear that the provisions on satisfying record retention rules with electronic documents do not authorize the destruction of documents originally received in paper form by government (any body subject to the freedom of information statutes) before they may be destroyed according to otherwise applicable record destruction schedules. [FN184] The Information and Privacy Commission took the view that access to the paper document was separately valuable to members of the public, even if all the information in it were contained in an electronic version of it.

(ii) Manitoba's Legislation

Part 2 of Manitoba's *The Electronic Commerce and Information Act* [FN185] deals with the "functional equivalence" rules, on how to satisfy writing, original and other requirements with electronic documents. Unlike the other provinces, but like the federal government, [FN186] Manitoba has enacted an opt-in scheme. The rules permitting electronic documents apply only to designated provisions of law. A positive action by government is needed to give them life. [FN187] Unlike the federal statute, the *Manitoba Act* does not require a regulation stating how the electronic document must be created to satisfy the legal requirement. The general standards of the *Uniform Act* apply once the provision is designated. Also, in contrast to the federal statute, the *Manitoba Act* does not provide for a centralized list or schedule of designations, so that people subject ***314** to Manitoba law could readily find out what provisions have been designated and are thus acceptable for electronic communications.

Manitoba's signature provision is even more restrictive. Not only must any communication be based on the consent of the parties - as in the *UECA* - and not only must the rule of law requiring a signature be designated before an electronic signature may satisfy it, but also any electronic signature must meet the reliability standard of the *U. N. Model Law* - that it be "as reliable as appropriate in all the circumstances." [FN188] This will lead to much doubt among signing parties whether what they choose as a signing technique will be valid in law, since a confident judgment in appropriateness will have to await court decisions, or further government direction.

At the date of writing, Part 2 is not in force, so no form requirements can yet be satisfied electronically in Manitoba under the new legislation.

Part 6 of the Manitoba statute amends the *Consumer Protection Act* to deal with Internet sales contracts. This part of the Act is discussed below in the Regulation section of this article. [FN189]

(iii) New Brunswick's Legislation

New Brunswick's *Electronic Transactions Act* [FN190] varies more dramatically from the *UECA* than do other provinces' implementing legislation. The main difference is its omissions: where the province considered that propositions went without saying, it did not say them. [FN191] Primary examples are in the authority for electronic contracting [FN192] and the special rules for documents for the carriage of goods, on which the *New Brunswick Act* is silent. This variation from the general Canadian practice may create questions of interpretation even though New Brunswick apparently does not intend any different result. It will be helpful if those called on to interpret the Act have recourse to the Consultation Paper. The *New Brunswick Act* also gives very broad authority to the Lieutenant Governor in Council to regulate "any ... characteristic of ***315** the electronic information that may or shall be used for the purpose of any provision of this Act or in relation to any matter." [FN193] Fine-tuning may come later, as the need arises.

Questions of principle influenced other omissions, such as any special provisions for documents coming into government. [FN194] In addition, New Brunswick has chosen to deal with what is excluded from the scope of

the Act by regulation only, unlike the *UECA*'s mix of legislative and regulatory choices. [FN195] A new consultation on exclusions was launched in September 2001. [FN196]

The *New Brunswick Act* runs contrary to the *UECA* in dealing with the deemed place of sending or receiving electronic messages. The *UECA* provides that such messages are deemed sent or received at the place of business of the sender or recipient. [FN197] New Brunswick says, "nothing in this section shall be interpreted as determining the place from which electronic information is sent nor the place at which it is received." [FN198] This may lead to unfortunate decisions that the place of the computer hardware or of an intermediary message service is relevant to the place of sending or receiving. It also means that the happenstance of where people are when they access their systems, or choices of electronic mail systems, will influence these decisions, even though the other party to the communication has no way of knowing these factors and thus the place that will ultimately be decided to be the one with legal effect. It thus becomes even more important under New Brunswick law than elsewhere for the parties to address their minds to questions of location and to agree ahead of time on them where they may be important to the transaction.

New Brunswick's rules on electronic signatures are consistent with those of the *UECA*, but the Act adds two examples of what may constitute ***316** an electronic signature, namely an electronic representation of the signer's manual signature, and electronic information by which the signer gives his or her name and indicates clearly that the name is provided as a signature. [FN199] Both of these methods fall within the definition in the *UECA*, [FN200] largely taken up by New Brunswick, [FN201] so it is not clear why this explanatory text was included in the statute rather than in supplementary material. The examples should not restrict the range of choices of signing methods effective under the Act.

Generally the *New Brunswick Act* is shorter than the *UECA* or other implementing legislation. The drafters have chosen to eliminate verbiage, even when the sense is not changed by the omission. [FN202] Again, this may lead to questions of intention that could have been avoided by following the uniform legislation more closely. It is fair to say that over time, lawyers and their clients are becoming more comfortable with the likely legal effect of electronic communications, and less detailed statutory help is thought necessary than a few years ago. The *UECA* reflects a balance of thinking on that subject as of late 1998, with some evolution thereafter. New Brunswick's statute reflects thinking two years later. On balance, the more economical version is unlikely to cause major concerns in practice. Some people may nonetheless regret that the province did not choose to avoid the additional questions caused by deviating for reasons of style only from the uniform legislation. [FN203]

(iv) Quebec's Legislation

Quebec adopted *an Act to establish a legal framework for information technology* in June 2001. [FN204] The Act is more ambitious than the ***317** *Uniform Act*. It shares with the *Uniform Act* the goal of technology neutrality, and of applying to all rules of law, not just commercial transactions. [FN205] It speaks of "technology-based" documents rather than "electronic" documents, but the definition of this term comes to about the same as the expansive sense given to "electronic" in the *Uniform Act*: "documentary communications using media based on information technology, whether electronic, magnetic, optical, wireless or other, or based on a combination of technologies." [FN206]

Quebec spells out more of the consequences of the use of technology than does the *Uniform Act*. For example, it contains four paragraphs about what a document is, [FN207] and several on how to track the integrity of the information in a document during its life cycle. [FN208] The stability of the content of the document is a primary concern of the Act. It is arguable that parties to electronic transactions governed by statutes implementing the *Uniform Act* will have to be sensitive to the same concerns as those stated in the

Quebec Act. Quebec does not leave the resolution of these concerns quite so much to the education or sophistication of the parties as does the *Uniform Act*, though both statutes leave open the means of achieving the appropriate degrees of assurance.

The Quebec statute spends nearly twenty sections on the link between a document and the person who originates it. This is the traditional role of a signature, but a signature is not the only evidence of the link. [FN209] In addition, the bill makes detailed provision for the activity of persons who certify the identity of signatories of technology-based documents and it sets up a voluntary accreditation scheme for them. It also examines the nature of recognized standards for reliable technology in this area. Further, Quebec provides for the liability, or the exemption from liability, of communications intermediaries such as Internet service providers.

In short, the approach taken by Quebec is considerably different from that of the *UECA*. It shows that a technology-neutral statute need ***318** not be minimalist. A number of critics have suggested that a more minimalist approach would have been preferable, though not all the critics have appreciated either the scope of the bill or the several parallels in principle to the *UECA*. [FN210] In any event, the Quebec bill can serve as a kind of user's guide to electronic communications, even for those under the less prescriptive legal regime of the *UECA*. At best, Quebec has given useful guidance for future work in the field to the common law jurisdictions in Canada.

(d) Federal Legislation on Electronic Documents

The Canadian federal government has passed the *Personal Information Protection and Electronic Documents Act*, known familiarly as PIPEDA. [FN211] The Act contains provisions on personal privacy, electronic documents and electronic evidence. Here we are concerned with Part 2 on electronic documents. [FN212] It came into force on May 1, 2000.

Part 2 of *PIPEDA* applies to provisions of federal statutes and regulations that impose or seem to impose paper requirements. The federal government mainly regulates interprovincial undertakings, such as broadcasting, telecommunications and railways, and certain prescribed sectors of the economy such as banks and some other financial institutions. Most smaller businesses are subject to provincial legislation. *PIPEDA* also applies, of course, to communications between members of the public - businesses or individuals - and the federal government itself. [FN213]

***319** The legislation permits federal government departments and agencies to use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information whenever a federal law does not specify the manner of doing so. [FN214] In other words, the general permission here yields to existing or future specific form legislation, just as the *UECA* does. [FN215] It also permits federal departments to make electronic payments as the Receiver General specifies. [FN216] Where forms are prescribed under federal law, electronic forms may be created or used for the purpose. [FN217]

Part 2 of *PIPEDA* sets up an opt-in scheme, by which certain media requirements can be met by electronic documents if the government department responsible for the requirement designates the requirement to be covered by the statute and if it makes regulations at the time of designation to say how the electronic documents are to be created or dealt with. The designated provisions will appear in Schedules to the Act - statutes in Schedule B, regulations in Schedule C [FN218] - so the public has a central point of reference to learn what provisions are in or out of the scheme. This method applies, for example, to writing requirements, [FN219] signatures, [FN220] copies [FN221] and the provision of information. [FN222]

This need for designation means that although the Part is "in force," most of it does not yet apply to anything, and will not until designations and regulations are made. The first such orders may be made later in 2002. It is likely that the rules for using electronic documents will be consistent with the principles of the *U. N. Model Law* and of the *UECA*.

However, the federal government has gone further than the *UECA* in one important aspect. Several sections of Part 2 contemplate the use of a "secure electronic signature." For example, one can use a secure electronic signature to create a certificate signed by a minister or public ***320** official that is proof of a fact or admissible in evidence. [FN223] A secure electronic signature may serve as a seal, if the seal requirement has been designated under the Act. [FN224] Affidavits may be made electronically if both deponent and commissioner of the oath sign with a secure electronic signature. [FN225] Declarations of truth may be made with such signatures, in similar circumstances. [FN226] Witnesses may sign under similar conditions. [FN227]

A "secure electronic signature" is not defined in the Bill, except as "an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1)." [FN228] That subsection sets out the usual provisions for signatures of this type, originally designed by the National Institute of Science and Technology (NIST) in the United States, [FN229] and since adopted or adapted in California, [FN230] Illinois [FN231] and other states, [FN232] and by *UNCITRAL* in its new draft Model Law on Electronic Signatures. [FN233] Similar language is found in the European Union Directive on Electronic Signatures mentioned above in the general section on signatures, [FN234] though there they are called "advanced electronic signatures." *PIPEDA* says [FN235] that a technology or process may be designated only if it can be proved (to the maker of the regulation, presumably) that:

> · the electronic signature resulting from the use by a person of the technology is unique to the person; ***321** · the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person; · the technology or process can be used to identify the person using the technology or process; · the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document. The intention is that in the first instance the only technology to be designated will be that of digital signatures certified by the Government of Canada, or those from systems cross-certified with the GOC PKI. [FN236] Some provincial governments are developing public key infrastructures as well, and they hope to be cross-certified with the federal PKI. This would help extend the reach of *PIPEDA*, since most provincial systems will probably issue digital signature certificates to a number of people in the private sector who could use them in dealing with the federal government as well (depending on the terms of the provincial implementation).

In short, the federal approach is a cautious one, but it does remove the major statutory barriers to electronic commerce. It does so by empowering the government to make regulations when and as appropriate. The law contains no encouragement to adopt harmonized standards across government, though it may be thought that that market forces and central planning of technology requirements will tend to harmonize the departments' approaches in any event. The *UECA* does not purport to harmonize the standards applicable to incoming documents among government***322** departments or agencies, either. Outgoing electronic documents would be subject to the general rules of functional equivalence. [FN237]

2. REGULATING ELECTRONIC TRANSACTIONS: CONSUMER PROTECTION

The state has a role in many aspects of electronic transactions, either actively to ensure values of public

policy, or passively through the court system to enforce or invalidate them. Only one has been the subject of widespread legislation in Canada: consumer protection. Industry Canada commissioned a study of the main legal issues in 1998. [FN238] A national consumer protection organization, the Public Interest Advocacy Centre (hereinafter *PIAC*), made a submission to all Attorneys General and all Ministers of Consumer Affairs in the country in June 2000, urging them to insert a list of consumer protection provisions into their versions of the *Uniform Electronic Commerce Act*. [FN239] To date none of the implementing provinces have picked up *PIAC*'s proposals, though Ontario's rule against "providing" legally required information on web sites and, arguably, the refined wording on implied consent reflect a few of the same principles.

In November 1999, a business/consumer task force published Guidelines on this subject, promoting education of all parties and standards for vendors and consumers engaging in on-line transactions. [FN240] They are similar to, but not directly influenced by, the American Bar Association guidelines for "safe shopping" published in October 1999. [FN241] They are intended to be consistent with consumer protection rules promulgated by the Organization for Economic Cooperation and Development (OECD). [FN242] In most of the country, the consumer protection rules remain only guidelines. However, legislative principles were developed by a federal-provincial-territorial (FPT) working group and adopted by ***323** Ministers from all jurisdictions in December 1999. [FN243] Here are the main legislative principles:

> · Consumer law should accept the use of electronic signatures where it requires contracts to be signed. · Electronic contracts should contain the prescribed disclosures (such as location of merchant, delivery and warranty terms, return and refund policies) and a "30-day delivery rule" by which if goods are not delivered within 30 days, the contract can be rescinded. The contract, including all required disclosures, should be given into the custody and control of the customer, e.g., by fax or download, and be printable. · Agreement to terms of a contract should be a clear process that a consumer cannot perform unwillingly. · Sellers should provide consumers with receipts as soon as possible after payment has been made. Receipts should be printed or be in printable form. · Purchasers should be able to cancel contracts for non-compliance with disclosure terms or for late delivery (as mentioned above). The point of this is that consumers' rights, including disclosure and remedies, would be substantially the same online as for transactions by traditional means.

Manitoba's electronic commerce legislation contains several non-uniform provisions to protect consumers. [FN244] They go mainly to disclosure and cooling-off periods. However, there are also rules for "Internet agreements" [FN245] that require credit card issuers to reverse consumer transactions in certain cases. [FN246] To date, these provisions have not drawn ***324** attention or criticism from financial institutions or anyone else. They came into force on March 19, 2001, together with complementary regulations. [FN247]

Ontario released a consultation paper on general consumer protection reform in the summer of 2000. The paper included a section on electronic commerce measures, mainly focused on disclosure rather than on regulation. The paper suggested that the province may introduce comprehensive legislation in the coming year. [FN248]

A federal-provincial-territorial working group reporting to ministers responsible for consumer measures has devised a "template" for legislative rules on consumer protection in "internet contracts." [FN249] The rules resemble Manitoba's statute and a draft circulated by Alberta in late 2000. [FN250] One of the elements to attract early discussion was the definition of "Internet sales contracts" themselves. In the days of convergence of media, did it make sense to try to separate out Internet transactions for individual treatment, or was it just too difficult to foresee the medium from which a message might come from or in which it might be read? Would it be preferable to attempt to find one set of rules apply to all transactions at a distance, or at least to those

conducted by electronic communications? To date the template has been implemented on its terms, i.e., limited to Internet sales. [FN251]

The template followed the legislative principles quite closely, as might be expected, requiring disclosure of essential terms and allowing rescission of a contract when the disclosure or delivery was defective. Credit card issuers were responsible for enforcing rescission when required by the consumer. Canadian jurisdictions will have the choice whether to enact these rules through legislation, regulation, or some ***325** combination of them. [FN252] The template did not, however, spell out just how the rules would apply, i.e., in what jurisdictions. The Alberta draft regulations had claimed effect where either the seller or the buyer was in Alberta, or where the message passed through an Alberta server at any time. It is difficult to see how any real interest of the enacting jurisdiction would be advanced by the latter rule. Further work on jurisdiction is under way, with a view to making a recommendation to responsible ministers in the spring of 2003. [FN253]

In the United States, consumer protection issues have taken a different focus. The national enabling statute for electronic transactions, the *Electronic Signatures in Global and National Commerce Act* (E-SIGN), [FN254] does not apply to certain kinds of communications with consumers. [FN255] For other consumer transactions, the Act requires clear evidence that the consumer is capable of communicating electronically with the merchant. [FN256] The debate continues about how many consumer-protection limits should be built into state legislation to implement the *UETA*, which itself does not have consumer protection provisions, except arguably the rescission right for mistakes in dealing with electronic agents. [FN257]

***326** The European Union has published reports on consumer protection in electronic commerce. The general distance selling directive of 1997 resembles the proposals for Canadian law. [FN258] The best known proposed rule would ensure that any consumer could have his or her own domestic law apply to an electronic financial transaction, and a dispute could be brought in his or her own court. Merchants in Europe have expressed concern about this, as it exposes them to 15 different legal regimes in their own market. [FN259] The EU has also been active in promoting cross-border administrative and judicial assistance to consumers. One recent document requires countries to establish mutual recognition regimes for their consumer protection authorities. [FN260] Another allows states to restrict inflow of consumer-oriented information if the state considers the information to be harmful and the originating state does not take adequate measures to remedy the problem. [FN261] It is not clear whether Canada will be influenced by either American or European approaches in the near future.

3. ELECTRONIC EVIDENCE

The substantive rules of law may accommodate electronic commerce, but they will be of limited assistance to business people unless the records of the electronic transactions can be fairly placed before the courts and administrative tribunals when disputes arise. Some work has been done in Canada in recent years on the law of evidence, to ensure the appropriate admission of computer-generated records. [FN262] This part of the paper describes the main law reform efforts.

***327** In practice, the courts have not been slow to recognize that businesses and governments keep their records on computers. Very few cases have refused to admit evidence on the ground that it was in electronic form. [FN263] As a result, litigation lawyers have often taken the view that no law reform is needed to promote the admissibility of electronic evidence. However, lawyers who are called on to advise clients on record keeping systems or on business communications issues generally have been more enthusiastic about legislative support on this issue. Some of the questions need more certain answers, in their view. [FN264]

The Canadian law of evidence is largely based on the common law, except in Quebec. [FN265] However, it

is supplemented extensively by statutes at the federal and provincial (and territorial) levels. The *Canada Evidence Act* [FN266] applies to proceedings under federal statutes, notably the Criminal Code of Canada [FN267] and in federally constituted administrative tribunals. Provincial evidence statutes [FN268] govern civil proceedings in court and matters before provincially constituted administrative tribunals. The Civil Code of Quebec has a part on evidence, [FN269] which applies to the same matters as the evidence statutes in other provinces.

Electronic evidence, for the purposes of this discussion, refers to evidence of computer-generated records, mainly business records. It is a form of documentary evidence, which, of course, the courts have been dealing with for a long time. [FN270] This article does not discuss computer ***328** simulations or computer-based analyses of statistics prepared for the purposes of particular litigation. These are forms of expert evidence to which quite different rules apply. [FN271]

(a) Principles of Documentary Evidence and Their Reform

Documentary evidence, including evidence in electronic documents, presents three legal problems. First, it is usually hearsay, rather than the direct testimony of a live witness under oath and available for cross-examination, which is the paradigm of good evidence in our court system. Second, such evidence needs to be authenticated, that is, identified in some authoritative way. Third, documents are subject to the "best evidence" rule, which generally requires that original documents be presented to the court, and that a good explanation be given if copies are to be admitted instead.

It should be noted that Canadian courts have not always kept these notions separate in their decisions. The tendency to merge the different concepts has made the area ripe for reform, in the view of the Uniform Law Conference's working group on electronic evidence. [FN272] The degree of confusion might have allowed ambitious and careful counsel the opportunity to exploit the inadequacies of the case law to create some serious difficulties in judicial doctrine and thus add to the uncertainty about what documents were admissible and why. To avoid such difficulties, the Uniform Law Conference adopted in 1998 the *Uniform Electronic Evidence Act*, [FN273] now in force in several jurisdictions. [FN274]

(i) Hearsay

The rules on hearsay are generally accepted to present no special problems for the admission of electronic records. The medium on which ***329** indirect evidence is stored does not alter the characteristics of that evidence as hearsay. As a result, the law dealing with the hearsay aspect of documentary evidence has been able to handle electronic records without difficulty. Indeed, the leading Canadian common law case on documents, *Ares v. Venner*, [FN275] set out rules that could be applied as well to electronic as to paper records. Statutory rules on documents have tended to follow. For example, the *Ontario Evidence Act* has a codification of the business records rule that defines "record" this way: "includes any information that is recorded or stored by means of any device." [FN276] This kind of thinking led the Uniform Law Conference of Canada to omit rules on hearsay from the *Uniform Electronic Evidence Act*. [FN277]

However, in the 1990s the Supreme Court of Canada made some important changes to the law of hearsay. The old rigid categories of exceptions to the rule, i.e., cases in which such evidence is admissible (such as business records), are disappearing. The more recent formulations of the Supreme Court say that hearsay evidence is admissible when it is "necessary and reliable." [FN278] The necessity of hearsay evidence is not usually difficult to demonstrate for documentary evidence, since the purpose of creating the documents in the first place is to preserve information beyond the capacity of human memory. Its reliability can be more contentious. However, documentary evidence has at common law been admitted on the ground that the manner in which it is created gives a "circumstantial guarantee of trustworthiness." [FN279]

Electronic documents may tend to reopen the debate, however. The impermanence and the malleability of information in electronic form ***330** make some electronic records unreliable. Others are, of course, thoroughly trustworthy, and technology offers many ways to give different degrees of assurance to them. It has been argued in Canada that the combination of electronic records and the restatement of the law of hearsay makes it necessary to develop new rules for the admission of such records in their character as hearsay. If these records are unreliable in different ways, then their reliability is a hearsay issue in a way it was not when that law was more bound in categories.

The main proponent of this point of view is Ken Chasse, who is much published on electronic evidence issues. [FN280] He would prefer that the courts examine in detail the circumstances of the creation and retention of electronic records. The recommendations of his 1994 paper echo the procedures of the Ontario Court of Appeal in *R. v. McMullen*. [FN281] This case has, however, been little followed since then.

The argument on the other side is twofold. First, the law does not investigate the actual abilities of the human beings that keep records, in order to apply the business records rule. Why should it investigate the inner workings of a computer? Second, "[t]he required circumstantial guarantee of trustworthiness flows from the presumption that businesses will create *systems* which ensure the reliability of their records. The nature of those systems, whether they involve computers or human beings, does not affect the reliability of that presumption." [FN282] (We are not talking here of records created with the prospect of litigation.)

As noted, the *Uniform Electronic Evidence Act* tends to the latter argument, at least in respect of hearsay, rather than Ken Chasse's more demanding recommendations. The debate is a reminder of the difficulty caused by using the same word "reliability" in several different contexts. It does not mean the same thing, or involve the same tests, when we are talking about authentication or best evidence. The quotation from Douglas Ewart's book in the preceding paragraph introduces yet another ***331** concept, of the reliability of a presumption (in effect, of reliability)! The *Uniform* Act tried to stay away from the word, if not the concept.

(ii) Authentication

In the law of evidence, a document must be authenticated before it can be admitted. Authentication means the demonstration of what a document is and where it came from. There must be evidence, generally live and under oath, to authenticate a document. However, in practice this foundation evidence does not need to be extensive. The usual formulation is that it must be "sufficient to support a finding that the document is what it purports to be." [FN283] One will note that the foundation evidence does not have to prove that the document *is* what it purports to be. That is a question of weight, after admission. Canadian reported cases have seldom dealt at length with authentication. It seems, however, that wide-ranging inquiries about the reliability of a document do not often occur at the authentication stage. The question for law reformers was whether electronic documents needed an additional test under this head.

The *Uniform Electronic Evidence Act* says no. On authentication it simply codifies the common law requirement noted above, that the foundation evidence be capable of supporting a finding of authenticity. [FN284] The intention, according to the commentary to the *Uniform Act*, is that the reliability of an electronic record should be tested only once to get the record admitted. This would happen under the rubric of the best evidence rule. [FN285] Whether the wording of the *Uniform Act* will be sufficient to impose that limit remains to be seen.

(iii) Best Evidence Rule

The third rule about documentary evidence, and indeed about all evidence, is that it must be the "best evidence" available. For documents, this has come to mean that the court wants to see an original document, or

have a good explanation of why the original is not available. The problem with electronic documents is that the concept of “original” does not apply very easily, for at least two reasons. First, electrons are manipulated***332** in many places to create a document, and they will leave traces, if not the whole document, in many of them. The random-access memory, the hard drive, disk drives, network backup tapes, and home as well as office computers - and one's colleagues' computers, if one can share screens during creation - can all be sites of electrons constituting the document. One is not necessarily more “original” than the other.

The second reason that “original” applies poorly is that copies are not distinguishable from the electronic file first created. The reason that a court (or anyone else) would want an original is to test its integrity. It is thought that changes will be easier to detect if they have been made on an original document. This makes sense for a text on paper, especially if written in ink by a pen. It does not make much sense for an electronic document. Electronic documents are made up of bits, which are mere instructions to run or not run an electric current. One version of an electronic document is likely as accurate as another, or just as likely to contain an alteration. (There are ways to increase one's confidence in the integrity of an electronic document, but they depend on its handling, not on its status as an original.)

Canadian courts have not always faced the best evidence rule in dealing with computer-generated records, and when they have done so, they have not been consistent. Some cases have found that the “original” was in a hard drive or central core of a mainframe computer, so the court had to be content with a copy printed out. [FN286] Others have found that the printout was a display of the original that satisfied the demand for an original. [FN287] The courts do not seem to have considered an electronic document shown to the court on a computer monitor from the “original” storage medium.

The *U. N. Model Law* on Electronic Commerce [FN288] provides that the admissibility of information shall not be denied on the sole ground of its electronic form, or on the ground that it is not in its original form, “if it is the best evidence that the person adducing it could reasonably be expected to obtain.” This last part is in effect a restatement of the common law rule. Its formulation may have undesirable consequences, however. Someone who made electronic images of paper records could ***333** arguably not introduce the images into evidence without having destroyed the paper, since the courts may be inclined to consider the paper as the best evidence, if the paper is available. It may still be open to the proponent of the evidence to demonstrate that the images are as good as paper, but why should that be necessary? If the images can be demonstrated to be reliable, the paper should become irrelevant. One can destroy it to save storage costs, or keep it for historical reasons, or destroy parts and keep parts. [FN289] This is not a question that should be resolved by the law of evidence.

The *Uniform Electronic Evidence Act* follows the principle of Article 8 of the *U. N. Model Law* on originals generally, which makes clear that the policy function of requiring an original is to help ensure the integrity of the record, i.e., that it has not been altered. The *Uniform Act* says that for an electronic record, the best evidence rule is satisfied “on proof of the integrity of the records system in or by which the data was recorded or stored.” [FN290] Note that it does not speak of “reliability”! In many cases there will be no other way to get at the integrity of the record than by referring to the system. The main other way to show integrity would be to have someone attest that the information in the record was accurate. However, if one had a live witness who could testify about the content of the document, one would not need the document. One could show integrity of a particular record by showing it had been securely encrypted in an appropriate way, but the encryption system is more likely to be part of a security system than devised for a single record. [FN291]

The integrity of the record-keeping system is not of course a guarantee of integrity of the individual record. However, the original nature of a document is also not a guarantee of its integrity. The best evidence rule works towards integrity, but does not ensure it. The drafting team for the *Uniform Act* wanted to replace the search for

original with some ***334** equivalent hurdle to admissibility, but the team did not intend to make admission of evidence much more difficult than it should be, given the nature of electronic records. For this reason, i.e., to avoid a lot of litigation on matters that would normally not be disputed, the *Uniform Act* contains a number of presumptions of integrity of a records system. The general presumption appears in section 5(a). The presumption is established 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, that the fact of its not operating properly did not affect the integrity of that electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system. [FN292]

The second provision of section 5 creates a presumption of integrity of the records system if the record was recorded and stored by a party to the proceedings adverse in interest to the proponent of the record. It is hard to show the integrity of someone else's system. The person best able to demonstrate the lack of integrity is the person whose record it is. If a person claims that a record recorded and stored by it has no integrity, let that person prove that lack (or rebut the presumption at least.) The presumption is limited to adverse parties, in order to prevent parties with the same interest from colluding by introducing each others' records to get the presumption.

The third provision creates a presumption in favour of the system of a stranger to the proceedings who created the record in the ordinary course of business. Bank records might be part of such a class. However, the records must not have been created or stored under the control of ***335** one of the parties, since that would call into question the independence that justifies the presumption. If the third party did create them under the control of the proponent, then the proponent should be able to fulfil the conditions for the first presumption, about the proper operation of the computer.

What is the strength of the presumption? The *Uniform Act* leads off section 5 with “in the absence of evidence to the contrary.” To rebut the presumption the other party must bring evidence against the presumption, but need not disprove it. Once the presumption is rebutted, or if it cannot be established in the first place, both sides would have to bring evidence to allow the court to decide whether the record-keeping system had sufficient integrity to justify admitting the record.

They can do this by reference to standards for the relevant system. The *Uniform Act* authorizes the court to consider “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.” [FN293] Standards could be national technical standards, practices current in a particular industry, usages unique to the party seeking admission of its document, or rules agreed to by trading partners in an electronic data interchange relationship. The credibility of the standards is a matter for argument.

Canada has a national standard, approved by the Canada General Standards Board (“CGSB”), on Microfilm and Electronic Images as Documentary Evidence. [FN294] This is a complex standard that incorporates by reference a number of subsidiary standards, some of them American. One of the terms of the standard, adopted in 1993, is that it be reviewed for technical accuracy every five years. A working group of the CGSB has recently proposed very minor changes to this standard. [FN295] More important, the group is developing a general standard for the admissibility of electronic records in general, and not just imaged records. This work is nearing completion.

***336** Before leaving the subject of the best evidence rule, one should consider subsection 4(2) of the *Uniform Act*:

> An electronic record in the form of a printout 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. The general definition of "electronic record" includes a printout of the information in the record. [FN296] This makes sense in general for evidence purposes, since the printout is often only the display of what is in the computer. What is in the computer may be the issue before the court. However, sometimes a document is created on a computer and printed and always used in its paper form. Most business correspondence falls into this class. Typewriters are rare in the modern office. Correspondence on paper is not. These letters are used at all material times as paper documents. If their content is at issue in a suit, it is the content of the letter, not the content of the computer where it originated, that is to be proved. The printout should be treated the same as a typewritten letter. Subsection 4(2) intends to ensure that result. The reasoning is supported by the decision of the Ontario Court of Appeal (upheld by the Supreme Court of Canada) in *R. v. Bell*, [FN297] where printouts of bank ledgers were held to be original records when the computer records had been erased and the paper records stored and relied on by the bank. The bank's reliance in practice on the paper records was the key to the decision, more than the absence of the electronic version.

It should be noted that this reasoning applies only to the law of evidence. For electronic communications generally, it does not make sense to include a printout in the concept of such communications. [FN298] The *UECA*, as noted earlier, is built on the distinction between documents in writing and documents in electronic form.

***337 (b) Law Reform on Electronic Evidence**

The Government of Canada was the first to introduce the *Uniform Act* into legislation. Part 3 of the *Personal Information Protection and Electronic Documents Act* [FN299] enacts the *Uniform Act* with a few changes in wording and structure to accommodate it to the *Canada Evidence Act*, where the Bill makes it section 31.1. The principal difference is that *PIPEDA* inserts the possibility of establishing "evidentiary presumptions" of integrity and source, where electronic records have been signed with a "secure electronic signature." [FN300] These presumptions can be brought into force by regulation, but none has been made at the time of writing.

Ontario adopted the *Uniform Electronic Evidence Act* almost verbatim, as a new section of the *Ontario Evidence Act*. [FN301] As noted earlier, Ontario has also expanded its provisions to allow for proof of integrity of electronic records through the use of encryption. [FN302] Saskatchewan passed its version of the *Uniform Act* in June 2000. [FN303] It came into force on November 1, 2000. Manitoba's electronic commerce statute, mentioned earlier, [FN304] deals with evidence too, in Part 7. While it is mainly drawn from the *Uniform Act*, it also picks up the federal statute's references to evidentiary presumptions based on secure electronic signatures. It came into force on October 23, 2000. The Yukon passed the *Uniform Electronic Evidence Act* in December 2000, [FN305] and it came into force on royal assent. Prince Edward Island did likewise in May 2001. [FN306] Alberta has enacted the *Uniform Act* as part of its *Electronic Transactions Act*. [FN307]

***338** Two non-uniform statutes are worth noting. The first is the Civil Code of Quebec, in effect on January 1, 1994. [FN308] Article 2837 says:

> A writing can be used to adduce proof whatever its medium. However, in order for a technology-based document to be the equivalent to a paper document, its integrity must be ensured as provided for in the Act to establish a legal framework for information technology. Article 2838 contains presumptions:
>
> The reliability of the entry of the data of a juridical act on a computer system is presumed to be sufficiently guaranteed where it is carried out systematically and without gaps and the computerized data

are protected against alterations. The same presumption is made in favour of third persons where the data were entered into by an enterprise. There appears to be no significant jurisprudence on these articles.

The second relatively recent item of law reform is the *Electronic Evidence Act* of New Brunswick. [FN309] This inserts into the provincial evidence statute a new section dealing with data evidence and electronic images. It sets up a system of affidavit support for the electronic evidence. Electronic images are admissible only if the paper originals have been destroyed in the usual course of business. It is arguable that in practice, affidavits about the creation and verification of the electronic records will not be available to cover the lifetime of the records, as distinct from the proceedings at the time of their creation, and some weight will need to be given to the reliability of the record-keeping system as well as of the affidavits, or the affidavits will have to deal with this element of the record's history too.

4. CONCLUSION

Canada's legal system is evolving to accommodate the disappearance of paper from so many of our legal relationships (if not from our businesses and law offices). The common law is managing to deal with much of the change, and legislation at federal, provincial and territorial levels aims to increase the legal certainty and thus the confidence of Canadians to engage in electronic commerce. The main legislative developments have affected electronic transactions, electronic evidence and individual privacy. [FN310]

***339** Canada is very sensitive to the global nature of electronic commerce, and to its relative size. As a result, it participates actively in developing international standards and promotes harmonization efforts at home as well. Through the Uniform Law Conference of Canada and otherwise, its various governments are working to ensure the greatest compliance possible with the best principles and best practices for the legal framework for electronic commerce. We share with the rest of the world the recognition that this is a work in progress.

[FNa1]. John D. Gregory, General Counsel, Policy Branch, Ministry of the Attorney General (Ontario), Canada. The views expressed here are not necessarily those of the Ministry of the Attorney General.

[FN1]. Questions of electronic evidence are dealt with *infra* in the text accompanying n. 262ff.

[FN2]. See A. H. Boss, "Searching for Security in the Law of Electronic Commerce" (1999), 23 Nova L.R. 585.

[FN3]. (1999), 40 C.P.C. (4th) 394, 1999 CarswellOnt 3195, [1999] O.J. No. 3778, 47 C.C.L.T. (2d) 168, 2 C.P.R. (4th) 474 (Ont. S.C.J.), additional reasons at (1999), 1999 CarswellOnt 3570 (Ont. S.C.J.).

[FN4]. A survey of click-through cases appears in C. Kunz, M. DalDuca, H. Thayer & J. Debrow, "Click-Through Agreements: Strategies for Avoiding Disputes on the Validity of Assent" (2001), 57 Bus. Law. 401 (2001) [Nov 2001]. See also "The Enforceability of Webwrap Contracts" by Baker & McKenzie (written before the Rudder case) at the Uniform Law Conference of Canada web site, online at: <*http://www.ulcc.ca/en/cls/index.cfm?secW4&subW4i*>.

[FN5]. *Newbridge Networks Corp., Re* (2000), 48 O.R. (3d) 47, 2000 CarswellOnt 1401, 186 D.L.R. (4th) 188, 7 B.L.R. (3d) 136 (Ont. S.C.J. [Commercial List]).

[FN6]. The statutes of most Canadian jurisdictions are accessible on line through <*http://www.acjnet.org/cdn.law/statutes.cfm*>. Ontario statutes are online at <*http://www.e-laws.gov.on.ca*>. Federal statutes are online at: < *http://lois.justice.gc.ca*>.

[FN7]. R.S.O. 1990 c. H.17.

[FN8]. *Statute of Frauds*, R.S.O.1990 c. S.19.

[FN9]. See, for example, the *Sale of Goods Act*, R.S.O. 1990 c. S.1, s. 5. (Section 5 of the *Sale of Goods Act* was repealed by S.O. 1994, c. 27, s. 54)

[FN10]. See, for example, the *Consumer Protection A*ct, R.S.O. 1990 c. C.31, s. 19.

[FN11]. For example, *Interpretation Act*, R.S.O. 1990 c. I.11, and *Interpretation Act*, R.S.C. 1985 c. I-21.

[FN12]. *Interpretation Act*, Ontario, *supra*, n. 11, s. 29(1). The federal language is almost identical, though it adds "typewritten" to the list of inclusions. *Supra*, n. 11, s. 35(1).

[FN13]. It is also arguable that machine-readable documents may satisfy the policy purposes of a requirement that a text be in writing, even though they do not display words at all. Coded documents used for electronic data interchange (EDI) transactions are an example. The Interpretation Acts would not generally allow this result.

[FN14]. Department of Justice (Canada), "Consultation Paper on Facilitating Electronic Commerce: Statutes, Signatures and Evidence" (1998), online at: < *http://canada.justice.gc.ca/en/cons/facilt7.html*>.

[FN15]. Searches can be run at Ontario's E-Laws site, online at: <*http://192.75.156.68/search_E.asp?langWen*>.

[FN16]. S.O. 1994 c. 27 ss. 54 and 55.

[FN17]. S.O. 1991 c. 44.

[FN18]. R.S.O. 1990 c. P.10. The statutes to which the *Electronic Registration Act* applies are designated by regulation under that Act. See O. Reg. 759/93 and O. Reg. 13/99.

[FN19]. *Land Registration Reform Act*, R.S.O. 1990 c. L.4, as amended by S.O. 1994 c. 27 s. 85.

[FN20]. *Business Regulation Reform Act*, S.O. 1994 c. 32, especially. s. 10.

[FN21]. *Business Electronic Filing Act*, S.N.S. 1995-96 c. 3; S.Nfld 1997, c. B-12.

[FN22]. *The Business Paper Reduction Act*, S.B.C. 1998 c. 26.

[FN23]. *The Electronic Filing of Information Act*, S.S. 1998, c. E-7.21 (now merged with the *Electronic Information and Documents Act*, S.S. 2000 c. E-7.22.)

[FN24]. See J. D. Gregory, "Solving Legal Issues in Electronic Commerce" (1999), 32 Can. Bus. L.J. 84 for further discussion.

[FN25]. *Offiicial Records of the 2*nd General Assembly, Fortieth Session, Supplement No. 17 (A/40/17). The text [hereinafter *U.N. Model Law*] and the very useful Guide to Enactment [hereinafter *Guide to Enactment*] are online at: < *http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm*.>

[FN26]. Useful sources of information on international developments in this field are the Internet Law and Policy Forum, online at: <*http://www.ilpf.org*>, the McBride Baker Coles firm web site, online at: <*http://*

www.mbc.com/ecommerce/international.asp>, and the Baker & McKenzie firm web site, online at: <*http://www.bmck.com/ecommerce/*>.

[FN27]. The texts are online at: <*http://www.law.upenn.edu/bll/ulc/ulc.htm #ueccta*> for the drafts and <*http:// www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm*> for the final version, and at: <*http://www.uetaonline.com*> for a record of the discussions leading up to its adoption and a list of states that have adopted it, with links to electronic versions of their legislation. For further analysis of the relation between international and domestic (U.S.) commercial law, see A. H. Boss, "Electronic Commerce and the Symbiotic Relationship between International and Domestic Law Reform" (1998), 72 Tulane L.R. 1931, and "The Uniform Electronic Transactions Act in a Global Environment" (2001), 37 Idaho L.R. 275.

[FN28]. [1999] Proceedings of the Uniform Law Conference of Canada 380, online at: <*http://www.ulcc.ca/en/us/index.cfm?secW1&subW1u1*>.

[FN29]. *Infra*, text accompanying n. 150ff.

[FN30]. *Guide to Enactment, supra* n. 25, para 51, 52. The power to exclude is set out as a potential exception to the application of particular articles, notably 6, 7, and 8.

[FN31]. *UECA, supra*, n. 28, s. 2(3)(d).

[FN32]. *UETA, supra*, n. 27, notably the Reporter's comments, "Legislative Note regarding possible additional exclusions under section 3(b)(4)," para. 3.

[FN33]. See the annotation to section 2 of the *UECA, supra*, n. 28.

[FN34]. *UECA, supra*, n. 28, s. 2(4). Some provincial implementing legislation differs in its treatment of negotiable or non-negotiable documents of title. The legislation is listed *infra*, n. 150.

[FN35]. More discussion of the reasons for exemption or inclusion in the *UETA* can be found in the report of a special committee that reported to the drafting group in the U. S., available online at: <*http:// www.webcom.com/legaled/ETAForum/docs/report4.html*>.

[FN36]. Department of Justice, New Brunswick, 2000, online at: <*http:// www.gnb.ca/justice/electronic-ev.doc*> [hereinafter *N.B. Consultation Paper*]. Most of the paper is a section-by-section commentary on the *UECA*, so the comments of the Department can be found together with the relevant section of the *Uniform Act*. The discussion of exclusions is found in the commentary on section 2 of the *UECA*.

[FN37]. New Brunswick's legislative approach to exclusions is discussed *infra*, text accompanying n. 190ff.

[FN38]. *N.B. Consultation Paper, supra*, n. 36.

[FN39]. See the annotation to section 2 of the *UECA, supra*, n. 28.

[FN40]. *Supra*, n. 19. Operational details are at <*http://www.teranet.on.ca*>.

[FN41]. See for example the *Land Title Amendment Act*, S.B.C. 1999, c. 35, creating Part 10.1 (s. 168.91) of the *Land Title Act*, R.S.B.C. 1996 c. 250, which deals with electronic filing. (The new part is not yet in force).

[FN42]. W. H. Hurlburt, "Electronic Wills and Powers of Attorney: Has their Day Come?" [2001] Proceedings

of the Uniform Law Conference of Canada, online at: <*http://www.ulcc.ca/en/poam2/e-wills-power-attorney.pdf*>. For the decision to keep the topic to a question of substantial compliance with form requirements, see the Resolutions of the Civil Section, 2001, online at: <*http://www.ulcc.ca/en/poam2/index.cfm?secW2001&subW2001g*>.

[FN43]. *UECA, supra*, n. 28, s. 2(5).

[FN44]. *Ibid.*, s. 2(7).

[FN45]. *UECA, supra*, n. 28, s. 2(2), 2(6).

[FN46]. *N.B.Consultation Paper, supra*, n. 36. This approach was taken in the New Brunswick legislation, *infra* n. 150. The annotation to section 2 of the *UECA, supra*, n. 28, says this: "While each enacting jurisdiction may choose the legal tool by which the list [of exceptions] may be made and amended, the action should be public, as is suggested by the bracketed term 'statutory instrument' [in s. 2(2) and (6)]."

[FN47]. *UECA, supra*, n. 28, s. 5. The double negative is used because information may be denied legal effect for any number of reasons besides its form, and the *UECA* does not affect such reasons. Some implementing statutes say "information to which this Act applies" and others simply say "information". It is not clear that this makes any difference in practice. A list of implementing legislation appears *infra*, n. 150.

[FN48]. *U. N. Model Law, Guide to Enactment, supra*, n. 25, para 43.

[FN49]. *UECA, supra*, n. 28, s. 6. The *UECA* says only that the Act does not require anyone to use information in electronic form. Most but not all of the provincial implementing legislation (*infra*, n.150) adds the phrase "without consent". The added phrase is intended as clarification but not as creating any difference in principle, since the *UECA* itself goes on to refer to implying consent. Only the *New Brunswick Act, ibid.*, s. 3, omits any express reference to consent, restricting itself to the absence of a requirement to use electronic information.

[FN50]. *UETA, supra*, n. 27, s. 5. The non-application of the U.S. Act in the absence of consent may cause difficulties where one needs to rely on its authority to do things not directly affecting other parties, such as setting up an electronic system for keeping records of transactions.

[FN51]. No. 162, 1999. Online at: <*http:// www.law.gov.au/publications/ecommerce*>. See, for example, ss. 9(1)(d) and 10(1)(d).

[FN52]. The *UETA, supra*, n. 27, provides in subs. 5(c) that a party who consents to conduct a transaction electronically may refuse to conduct other transactions by electronic means. Comment 5 to that section notes some limits to this right of refusal. The *UECA, supra*, n. 28, is silent on the point, but the policy is not likely to be held to differ.

[FN53]. If an electronic document is "writing" under the *Interpretation Act*, then one could arguably avoid the need for consent for the use of such a document. However, since the electronic commerce statutes are drafted to distinguish between writing on one hand and electronic documents on the other (*infra*, text at n. 63), the better view seems to be that the Legislature has expressed a contrary intention and the Interpretation Act meaning will not apply.

[FN54]. *UECA, supra*, n. 28, s.2. This formulation leaves open an interesting question whether provisions of federal law effective in the jurisdiction would be covered. The question arises in part because of proposed

amendments to the Criminal Code of Canada. These amendments allow courts, in applying the Code, to deal with electronic documents "in accordance with an Act" (proposed s. 842 of the Code) and to accept transfers of data done electronically if they are done "in accordance with the laws of the place where the transfer originates or the laws of the place where the data is received" (proposed s. 843 of the Code). S. 2 of the Code includes provincial legislation in the definition of an Act. Criminal Law Amendment Act, 2001, Bill C-15A, third reading October 18, 2001, online at: <*http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-15A/C-15A_3/98148b_5e.html*>. Some provincial implementing legislation may be clearer on this point than others. See a list of the provincial statutes *infra*, n. 150.

[FN55]. See, for example, *U. N. Model Law*, *supra*, n. 25, art. 6(2), 7(2), and others.

[FN56]. *Electronic Transactions Act* (Australia), *supra*, n. 51, for example ss 9(2) and 11(2).

[FN57]. *UECA*, *supra*, n. 28, s. 4.

[FN58]. The concept of functional equivalents is explained in more detail in the *Guide to Enactment*, *supra*, n. 25, para. 15ff.

[FN59]. *UECA*, *supra*, n. 28, s. 7. The wording tracks *U.N. Model Law*, *supra*, n. 25, art. 6.

[FN60]. See the introductory annotation to the UECA, *supra*, n. 28, fifth para. This principle too is inherent in the *U. N. Model Law*. See *Guide to Enactment*, *supra*, n. 25, para 16.

[FN61]. *UECA*, *supra*, n. 28, s. 13. While the *UECA* is silent on the point, people who keep electronic records for legally prescribed periods will presumably have to update their storage hardware and software from time to time if that is necessary for the record to be accessible for as long as required. The special needs of archivists are beyond the scope of this article.

[FN62]. Compare *Guide to Enactment*, *supra*, n. 25, para. 50.

[FN63]. *Infra*, n. 150.

[FN64]. The author chaired the working group that developed the *UECA*.

[FN65]. See for example *UETA*, *supra*, n. 27, s. 7(c): "If a law requires a record to be in writing, an electronic record satisfies the law."

[FN66]. *Ibid.*, s. 2(13).

[FN67]. For a discussion of the principles in the term "record", see Patricia B. Fry, "X Marks the Spot: New Technologies Compel New Concepts for Commercial Law" (1993), 26 Loyola L.A. Law Rev. 607.

[FN68]. *UECA*, *supra*, n. 28, s. 1. Compare the Quebec new technologies statute, *infra*, n. 204, which devotes four paragraphs in ss. 3 and 4 to saying what a document is. Some provincial implementing statutes have attempted to clarify the relation between information and documents. Saskatchewan called its statute the *Electronic Information and Documents Act*, *infra*, n. 150. It is arguable that the difference does not matter to how the *UECA* operates.

[FN69]. *Electronic Transactions Act*, Australia, *supra*, n. 51, s. 5(1), definition of "electronic communication":

"(b) a communication of information in the form of speech ... where the speech is processed at its destination by an automated voice recognition system." The American federal legislation, *E-SIGN*, *infra*, n. 87, s. 101(c)(6), provides that oral communications are not covered as electronic records, but their legal status is left to other law. The definition of "electronic record" in the *UETA*, *supra*, n. 27, appears broad enough to cover them.

[FN70]. *UECA*, *supra*, n. 28, ss. 8(1)(a), 9(1)(a), and elsewhere (as well as meeting the general requirement to serve as writing, that it be accessible for subsequent use.) The *UECA* does not say whether all recipients have to be capable in fact of retaining, or whether there is some objective standard of a recipient with reasonably foreseeable equipment and computer skills. Some reasonableness test is likely, but it may depend on the importance of the information to the recipient as well. The more important the information, the easier it may have to be to retain the information. Note the additional qualification in *UECA* s. 12 that a document is not capable of being retained if the sender of the document inhibits its printing or storage.

[FN71]. For further discussion of this point, and of Ontario's language elaborating on it, see *infra* text accompanying n. 165.

[FN72]. *UETA*, *supra*, n. 27, s. 8(a), which says "an electronic record capable of retention".

[FN73]. See August 1998 draft of *UECA*, in the Proceedings of the Uniform Law Conference, online: <*http://www.ulcc.ca/en/poam2/index.cfm?secW1998&subWWW1998ja*>. The federal legislation, discussed *infra*, n. 211, uses the language of control for this purpose in s. 40(c).

[FN74]. *UECA*, *supra*, n. 28, s. 9. Ontario and B.C. say "organized in substantially the same way," for drafting reasons. A list of provincial implementing legislation appears *infra* n. 150.

[FN75]. Compare the regulations on electronic documents under Ontario's Provincial Offences Act, R.S.O. 1990 c. P.33, at O. Reg. 497/94, s. 1: "A document is properly completed in an electronic format if the information provided, (a) is intelligible in a form prescribed under the Act when that information is used for any purpose under the Act; and (b) cannot be altered after the document has been signed electronically, except for the elaboration of coded information or its compression or encryption, or the addition of codes necessary for mailing it or for its proper submission ...".

[FN76]. *UECA*, *supra*, n. 28, s. 15.

[FN77]. See *UETA*, *supra*, n. 27, s. 8(b).

[FN78]. *N.B.Consultation Paper*, *supra*, n. 36.

[FN79]. *Ibid.*, discussion of section 15 of *UECA*, *supra*, n. 28. However, New Brunswick's legislation, *infra*, n. 150, contains two sections on meeting mailing requirements with electronic documents (ss. 13 and 14).

[FN80]. Further examples are given in J. D. Gregory, "The *UETA* and the *UECA*: Canadian Reflections" (2001), 37 Idaho L.R. 441.

[FN81]. *UECA*, *supra*, n. 28, s. 1(b).

[FN82]. *UETA*, *supra*, n. 27, s. 2(8).

[FN83]. C. Reed, "What is a Signature?", 2000 (3) *Journal of Information, Law and Technology (JILT)*, online at: <*http://elj.warwick.ac.uk/jilt/00-3/reed.html*>.

[FN84]. The *UETA*, *supra*, n. 27, says that an electronic signature is a "sound, symbol or process" (*ibid.*), though "result of a process" might be a more accurate parallel to sound or symbol.

[FN85]. *UECA*, *supra*, n. 28, s. 10.

[FN86]. *U. N. Model Law*, *supra*, n. 25,art. 7(1).

[FN87]. *UETA*, *supra*, n. 27, s. 7(a). While the *UETA* does not impose additional requirements on electronic signatures, the U. S. federal legislation of June 2000, the *Electronic Signatures in Global and National Commerce Act* [hereinafter *E-SIGN*] does limit its application in respect of several kinds of consumer transaction. See the section on consumer protection, *infra*, text accompanying n. 238. Otherwise *E-SIGN* prohibits state legislatures from enacting any rules for electronic signatures that would be more onerous, or more technology-specific, than the rules of the *UETA*, of which *E-SIGN* encourages the adoption. More on the complex relation of the US federal and state laws can be found online at: <*http://www.uetaonline.com*> and in S. Meehan & B. Beard, "What Hath Congress Wrought? E-Sign, the *UETA* and the Question of Pre-emption" (2001), 37 Idaho L.R. 389. *E-SIGN* itself , Public Law 106-229, June 30, 2000, can be found online at: <*http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbnameW106_cong_public_ laws&docid+f:publ229.106.pdf*>.

[FN88]. See, for example, *Fredericton Housing Ltd. v. R.*, [1973] C.T.C. 160, 1973 CarswellNat 122, 1973 CarswellNat 324, [1973] F.C. 196, 73 D.T.C. 5145 (Fed. T.D.), affirmed 1973 CarswellNat 161, 1973 CarswellNat 337, [1973] F.C. 681, 40 D.L.R. (3d) 392, [1973] C.T.C. 400, 73 D.T.C. 5329 (Fed. C.A.).

[FN89]. Whether the words "I agree" can themselves constitute a signature is a question of the intent of including those words in a message. Generally they would be evidence of consent to a transaction, or whatever document they were appended to, but not a signature in themselves unless the context showed such an intent, e.g., "Sign below by clicking the icon 'I agree"'. The contract provisions of the enabling statutes, discussed *infra*, n. 121, deal with demonstration of intent to contract rather than with signature as such.

[FN90]. The appropriate expression is "permit the identification of the signer" rather than "identify the signer". A signature does not have to be a person's name. Even if it is a person's name, a valid handwritten signature may be illegible, and then it permits the identification of a person only with additional evidence. Electronic data that require additional evidence to identify the person that applied the data as a signature are not different in principle.

[FN91]. One can have sufficient evidence of identity of the source of a document without a signature at all, from the content or context or history of the document. One may be able reasonably to rely on an unsigned document, but rarely on a document whose origin is unknown. Such evidence of attribution may not satisfy a legal requirement that there be a signature, however. The point is that one should not exaggerate the importance of signatures in ordinary transactions. One may have to answer separately the formal question "is it signed?" - which the *UECA* allows to be answered positively by an electronic signature - and the practical question "who signed it?" See J.D. Gregory, "The Authentication of Electronic Legal Documents" (1999), 6 The E.D.I.L. Rev. 47.

[FN92]. *UECA*, *supra*, n. 28, s. 10(2).

[FN93]. See online at: <*http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf*>. For a Canadian viewpoint on the nearly-final text, see Department of Justice (Canada), "UNCITRAL Working Group on Electronic Commerce: Report on the Meeting of September, 2000", online at: <*http://canada.justice.gc.ca/en/ps/ec/un2000rep.html*>. Compare the European Union's Directive on Electronic

Signatures, Directive 99/93/EC, December 1999, online at: <*http://europa.int.eu/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf*>. It allows for reliable electronic signatures to be proved in any way. It goes on to prescribe in considerable detail a regime for "advanced electronic signatures" created by "qualified signature creation data" and supported by "qualified certificates". The result of using this technology is an electronic signature to which member states must give the legal effect of a handwritten signature. This may strike some as a weak result for a strong technology, though one can debate the ability of any particular technology to meet the criteria or to operate properly once the criteria have been satisfied.

[FN94]. *UECA, supra*, n. 28, s. 6.

[FN95]. *UETA, supra*, n. 27, s. 9(a).

[FN96]. *Australian Electronic Transactions Act, supra*, n. 51, s. 15.

[FN97]. The *Guide to Enactment* calls it a presumption; *supra*, n. 25 para. 83. *U. N. Model Law, supra*, n. 25, art. 13(3)(4).

[FN98]. Reports of the Drafting Committee meetings at the ETA Forum (the predecessor to the *UETA* Online site) can provide details. Online at: < *http://www.webcom.com/legaled/ETAForum/mtgrpts.html*>, notably the meetings of September 1997 and January 1998.

[FN99]. *Infra*, text accompanying n. 211.

[FN100]. See the reports of the meetings of *UNCITRAL*'s Working Group on Electronic Commerce, notably for July 1998 (A/CN.9/454, para. 40 - 53); for February 1999 (A/CN.9/457, para. 99 - 107, and Working Paper WP.79 para 31 - 33); for September 1999 (A/CN.9/465, para. 68 - 77); and for February 2000 (A/CN.9/467, para. 44 - 71). All are online at: <*http:// www.uncitral.org/english/workinggroups/wg_ec/index.htm*>.

[FN101]. The requirement for original documents under the "best evidence" rule is covered in the *Uniform Electronic Evidence Act*, a separate statute adopted in 1998. Evidence questions are discussed in Part 3 *infra*, text at n. 262ff.

[FN102]. Ontario's version of this provision divides the treatment of originals into two subsections, one for where they started on paper and the other for where they started in electronic form. The statute is discussed at more detail *infra* at text accompanying n. 158ff.

[FN103]. *UETA, supra*, n. 27, s. 12.

[FN104]. *UECA, supra*, n. 28, s. 14. This applies only where the person providing the copies is entitled to use electronic documents at all. It is not a way to avoid making copies of documents to be submitted on paper.

[FN105]. Quebec statute, *infra*, n. 204, s. 32.

[FN106]. *UECA, supra*, n. 28, s. 6(2).

[FN107]. *Ibid.*, ss. 7, 8, 10 and 12.

[FN108]. By implication, since the Act binds the Crown (*UECA, supra*, n. 28, s. 3) and no special rules are provided for outbound documents.

[FN109]. *Supra*, n. 51.

[FN110]. *UETA, supra*, n. 27, ss. 17 and 18.

[FN111]. *PIPEDA, infra*, n. 211, s. 48.

[FN112]. *UECA, supra*, n. 28, s. 6(2).

[FN113]. *UETA, supra*, n. 27, s. 19.

[FN114]. *UECA, supra*, n. 28, annotation to s. 1 (which leaves open to enacting jurisdictions whether to exclude some or all Crown corporations from the definition.)

[FN115]. Most but not all jurisdictions implementing the *UECA* have maintained the rules for government, and all who have done so have included municipalities as "government". See the discussion *infra*, text at n. 150ff.

[FN116]. Alberta is the only province to break the silence, expressly to exclude the courts from the term. *Alberta Act, infra*, n. 150, s. 1(1)(h)(ix).

[FN117]. *Electronic Transactions Act* (Australia), *supra*, n. 51, s. 13.

[FN118]. *E-SIGN, supra*, n. 87,s. 103(B)(1).

[FN119]. *UETA, supra*, n. 27, s. 2(9).

[FN120]. *UECA, supra*, n. 28, ss. 19 - 22. *U.N.Model Law, supra*, n. 25, art. 11 - 12.

[FN121]. *UECA, supra*, n. 28, s. 20.

[FN122]. Ontario, Manitoba and Alberta have expressly included speaking to the computer. See statutes listed *infra*, n. 150. Ontario s. 19(1)(b)(ii), Manitoba s. 19(1)(b), Alberta s. 27(b)(ii).

[FN123]. *UECA, supra*, n. 28, s. 19.

[FN124]. See I. R. Kerr, "Providing for Autonomous Electronic Devices in the *Uniform Electronic Commerce Act*" (2000), online at: <*http:// www.ulcc.ca/en/cls/index.cfm?secW4&subW4f.*>.

[FN125]. *UECA, supra*, n. 28, s. 21.

[FN126]. The rule here applies whether the individual is acting on his or her own behalf or on behalf of another legal entity, like a corporation.

[FN127]. *UETA* s. 10(2).

[FN128]. The *New Brunswick Act, infra*, n.150, s. 18(4), spells this out, as does the *UETA, supra*, n. 27, s.10(3).

[FN129]. Directive 2000/31/EC, on certain legal aspects of the information society services, in particular electronic commerce, in the internal market. It is online at: <*http://europa.int.eu/eur-lex/en/lif/dat/2000/en_300L0031.html*>. This Directive was to be implemented by member states by January 2002.

[FN130]. *U. N. Model Law* art. 15; UECA s. 23(1).

[FN131]. *Guide to Enactment, supra*, n. 25, para. 100.

[FN132]. *Guide to Enactment, ibid.*, says that article 15 is not intended to establish a conflict-of-laws rule. For more on this aspect of electronic messages, see J. D. Gregory, "Receiving Electronic Messages" (2000), 15 B.F.L.R. 473.

[FN133]. The *OECD* has recently published guidelines on this question, online at: <*http://www.oecd.org/daf/fa/e_com/public_release.htm*>.

[FN134]. Jurisdiction questions are beyond the scope of this article. For an overview of case law, particularly U.S. case law, see B. Sookman, Computer, Internet and Electronic Commerce Law (Toronto: Carswell, 2000) ch. 11. For a recent analysis of private law jurisdiction, see M. Geist, "Is There a There There?: Toward Greater Certainty for Internet Jurisdiction", Uniform Law Conference of Canada, 2001, online at: <http://www.ulcc.ca/en/cls/internet-juridiction.pdf>. Public law jurisdiction is reviewed in R. Tassé & M. Faille, "Online Consumer Protection: A Study of Regulatory Jurisdiction in Canada," Office of Consumer Affairs, Industry Canada, 2001, online at: <http:// www.ulcc.ca/en/cls/index.cfm?secW4&subWn>. See also Ogilvy Renault, "Jurisdiction and the Internet: Are the Traditional Rules Enough?", online at: <*http://www.ulcc.ca/en/cls/index.cfm?secW4&subW4h*>.

[FN135]. *UECA, supra*, n. 28, s. 23(1).

[FN136]. *U. N. Model Law, supra*, n. 25, art. 15(2). Proving that a message entered a system at a particular time can be challenging. Internet service providers have varying policies on how long they keep logs of messages.

[FN137]. *UETA* s. 15(b). Designating a system for a type of message may constitute consent to receive that type of message electronically.

[FN138]. *UECA, supra*, n. 28, s. 23(2). The *UECA* is unfortunately silent on the case where the addressee has designated a system but the message is sent to another system. Arguably, the right approach is to treat such a message like one sent when no system had been designated, so the message is not presumed received until the address has notice of and access to it. The language in the New Brunswick implementing statute seems to avoid this problem: *infra*, n. 150, s. 16(2).

[FN139]. *UECA, supra*, n. 28, annotation to s. 23. Consider a message that enters the addressee's system and is accessible, but then the system goes down and it stops being accessible. Has it been sent? Has it been received? These questions may have different answers (as can happen with normal paper messages.)

[FN140]. Designating a system does not stop someone from designating a different one later. The language of the *UECA* that the system be "designated or used" does not mean that any use of a system will effectively designate it forever. What one has to do to "de-designate" a system will depend on the situation and dealings of the parties.

[FN141]. Could parties to a transmission agree that messages were sent when posted on a named web site, for example, and thus avoid other rules in the legislation about how messages must be sent (such as the rules about providing information)? The answer may depend on the language of the rule that requires the provision of the information.

[FN142]. It was not thought necessary in the *UECA* expressly to exclude the mailbox rule, by which an acceptance of a contract is deemed received when it is mailed not when it is received. I submit elsewhere that the mailbox rule should not apply to any electronic messages. See J. D. Gregory, "Receiving Electronic Messages," *supra*, n. 132. The *Uniform Act* applies to all communications, not only to the acceptance of offers of contract. The *U. N. Model Law*, *supra*, n. 25, art. 14, deals with acknowledgements, but the Uniform Law Conference working group did not think it said anything worth legislating in Canada.

[FN143]. *U. N. Model Law*, *supra*, n. 25, art. 16 and 17.

[FN144]. *Guide to Enactment*, *supra*, n. 25, para. 113, 118.

[FN145]. *UECA*, *supra*, n. 28, ss. 24 and 25.

[FN146]. *Ibid.*, s. 25(2).

[FN147]. Ontario's statute refines the language further without changing the concepts. See *infra*, n. 150.

[FN148]. *UETA*, *supra*, n. 27, s. 14.

[FN149]. See for example the work at <*http://www.e-original.com*>. The United States did provide for electronic warehouse receipts for shipments of cotton, before the current wave of e-commerce statutes. U.S.C. Title 7, s. 259.

[FN150]. In order of adoption: Saskatchewan, *Electronic Information and Documents*, S.S.2000 c. E-7.22, in force November 1, 2000, online at: <*http:// www.qp.gov.sk.ca/documents/English/Statutes/Statutes/E7-22.pdf*>, (*Electronic Information and Electronic Documents Amendment Act*, 2002, Bill 7, second reading April 17, 2002, online at: <*http:// www.legassembly.sk.ca/bills/PDFs/bill-07.pdf*>). Manitoba, *Electronic Commerce and Information Act*, C.C.S.M. 2000 c. E.55, in force October 23, 2000 (in part), online at: <*http://www.gov.mb.ca/chc/statpub/free/pdf/b31-1s00.pdf*>; Ontario, *Electronic Commerce Act*, 2000, S.O. 2000 c. 17, in force October 16, 2000, online at: <*http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/00e17_ e.htm*>; Nova Scotia: *Electronic Commerce Act*, S.N.S. 2000 c. 26, in force November 30, 2000; online at: <*http://www.gov.ns.ca/legi/legc/bills/58th_ 1st/3rd_read/b061.htm*>; Yukon: *Electronic Commerce Act*, S.Y. 2000 c. 10, in force March 27, 2001, online at: <*http:// www.economicdevelopment.yk.ca/publications/legislationRegs/Electronic%20Commerce%C .pdf*>; British Columbia: *Electronic Transactions Act*, S.B.C. 2001 c. 10, in force April 13, 2001; online at: <*http:// www.legis.gov.bc.ca/2001/3rd_read/gov13-3.htm*>; Prince Edward Island: *Electronic Commerce Act*, S.P.E.I.2000 c. 31, in force May 15, 2001, online at: *http://www.gov.pe.ca/law/statutes/pdf/e-04_1.pdf*; New Brunswick, *Electronic Transactions Act*, S.N.B. 2000 c. E-5.5, in force March 31, 2002, online at: < *http://inter.gov.nb.ca/legis/bills/54%2D3/070e.htm*.; Alberta, *Electronic Transactions Act*, R.S.A. 2000, c.E-E, 5, not yet in force, online at: <http:// www.assembly.ab.ca/pro/bills/ba-bill.asp?SelectBillW021>; *Newfoundland and Labrador Electronic Commerce Act*, S.N.L. 2001 c. E-5.2, in force December 13, 2001.

[FN151]. Quebec's statute is discussed *infra*, text accompanying n. 204.

[FN152]. *Supra*, n. 23; In its amendments proposed in 2002, *supra*, n. 150, Saskatchewan adds a definition of "public body" and integrates the concept with its electronic filing provisions.

[FN153]. *PEI Act*, *supra*, n. 150, s. 1(1)(b). The rules for use of electronic signatures are, however, the same as those of the UECA. *Ibid.*, s. 9.

[FN154]. The federal Act is discussed *infra*, text accompanying n. 211.

[FN155]. See the discussion of the legal acceptability of electronic signatures at common law, *supra*, text accompanying n. 81ff.

[FN156]. P.E.I. Legislative Assembly, Hansard, April 10, 2001, pp.1093-4, online: <*http://www.gov.pe.ca/leg/hansard/2001spring/2001-04-10-hansard.pdf*>.

[FN157]. One might speculate that PEI was influenced by the recent work of *UNCITRAL* on standards of reliability for electronic signatures, noted briefly *supra* at n. 90. Article 6 of the new Model Law on Electronic Signatures contains similar language, though in a more flexible context. See the report on the final draft of this Model Law, *supra* n. 93.

[FN158]. *Ontario Act*, *supra*, n. 150, s. 1(1) Manitoba and Alberta also say “public bodies” instead of the UECA's “government”.

[FN159]. *Ibid*., ss. 1(1)(c) and 32(a).

[FN160]. *Ibid*., s. 30.

[FN161]. For more on electronic voting, see the Internet Voting Technology Alliance online at <*http://www.ivta.org*>. The system used in Toronto's municipal election in 2000 counted electronically ballots marked by hand.

[FN162]. *Ontario Act*, *supra*, n. 150, s. 15(4) underlines that the Act does not authorize them to require people to use or accept information in electronic form. This is inherent in the general consent rule in the *UECA*. The provision would not invalidate some other source of such a requirement. The *Alberta Act*, *supra*, n. 150, s. 21, follows Ontario.

[FN163]. *Ontario Act*, *supra*, n. 150, s. 3(2). Alberta's Act follows this lead; see *Alberta Act*, *supra*, n. 150, s. 8(2).

[FN164]. Some of the limits of implied consent are explored in the Reporter's Notes to s. 5 of the *UETA*, *supra*, n. 27.

[FN165]. *Ontario Act*, *supra*, n. 150, s. 10. In its amendments proposed in 2002, *supra*, n. 150, Saskatchewan adds a similar limit on the provision of information, but appears to allow a proposed recipient to consent to provision by giving access. See s. 7 of the amending legislation, creating a new s. 13(2).

[FN166]. *Ibid*., s. 10(2)(a).

[FN167]. National Policy 11-201, “Delivery of Documents by Electronic Means”, online at: <*http://www.osc.gov.on.ca/en/Regulation/Rulemaking/Policies/11-201_19991215.html*>.

[FN168]. See, for example, Securities and Exchange Commission, SEC Interpretation: Use of Electronic Media, notice of proposed guidelines, online at: <*http://www.sec.gov/rules/interp/34-42728.htm#seciia*>.

[FN169]. *Ontario Act*, *supra*, n. 150, s. 26(1).

[FN170]. See the submission of the Canadian Bankers' Association to Ontario's Standing Committee on Justice

and Social Policy, August 28, 2000, online at: *<http://www.ontla.on.ca/hansard/37_ parl/ session1/Committees/justice/J021.htm#P296_123667>* at 1400 hours.

[FN171]. *Supra*, n. 18, s. 28(3) and (4).

[FN172]. *Ontario Act*, supra, n. 150, s. 8(4).

[FN173]. The American parallel to the PPSA, Article 9 of the Uniform Commerce Code, was amended in 1999 to deal with electronic records of secured transactions. See the documents online at: *<http:// www.law.upenn.edu/bll/ulc/ulc.htm#ucc9.>*. The Uniform Law Conference has given some consideration to similar work in Canada. See the annual proceedings of the Conference for 1999 and 2000, online at: *<http:// www.ulcc.ca/en/poam2/index.cfm?secW1999&subW1999jk>* and *<http:// www.ulcc.ca/en/poam2/index.cfm?secW2000&subW2000if>*.

[FN174]. *Nova Scotia Act, supra* n. 150, s. 12(3). Other versions of the P.P.S.A. appear to present similar difficulties, however. See, for example, the Alberta P.P.S.A., R.S.A. 2000 c.P-7, s. 31(4) and (5); the British Columbia P.P.S.A., R.S.B.C. 1996, c. 359, s. 31(4) and (6).

[FN175]. See *Ontario Act, supra*, n. 150, s. 11(4).

[FN176]. See *supra*, n. 25 and *UECA, supra*, n. 28, s. 10(2).

[FN177]. See the submission of the Canadian Bankers' Association to Ontario's Standing Committee, *supra*, n. 170, at 1410 hours.

[FN178]. For example, a seal may demonstrate an official source for a document, or help demonstrate its integrity, or attest to the status of the originator or commissioner (e.g., a notarial seal), or replace consideration on a contract as a demonstration of the intent of the parties to be bound.

[FN179]. *Ontario Act, supra*, n. 150, s. 11(6).

[FN179a]. The Ontario provision is s. 11(2).

[FN180]. *Infra*, n. 204, s. 10.

[FN181]. Biometric information is defined so as not to apply to photographic evidence or signature dynamics, as neither of these techniques lends itself well to finding a match for the person in a large database. They are best at confirming identity on a one-to-one comparison. *Ontario Act, supra*, n. 150, s. 29. cf. the *Alberta Act, supra*, n. 150, s. 5.

[FN182]. See online at: *<http:// www.cbs.gov.on.ca/mcbs/english.56hk6v.htm.http://www.cbs.gov.on.ca/>*.

[FN183]. *Ontario Act, supra*, n. 150, s. 27(1). Cf the *Alberta Act, supra*, n. 150, s. 3(1).

[FN184]. *Ontario Act, supra*, n. 150, s. 27(2). Cf the *Alberta Act, supra*, n. 150, s. 3(2).

[FN185]. *Supra*, n. 150.

[FN186]. See *infra*, text accompanying n. 211ff.

[FN187]. See for example the *Manitoba Act, supra*, n. 150, ss. 8 and 9.

[FN188]. See the *Manitoba Act*, supra, n. 150, s. 13(1).

[FN189]. *Infra*, text accompanying n. 238.

[FN190]. *Supra*, n. 150.

[FN191]. The legislation in effect follows most of the recommendations in the *N.B. Consultation Paper*, *supra*, n. 36.

[FN192]. *UECA*, *supra*, n. 28, s. 20.

[FN193]. *New Brunswick Act*, *supra*, n. 150, s. 19(1).

[FN194]. *UECA*, *supra*, n. 28, ss. 1, 6, 8 - 11 and 16 - 18. British Columbia also omitted special rules for government, as did Saskatchewan, which nonetheless has a separate part of its Act on filing with government. See the *Saskatchewan Act*, *supra*, n. 150, ss. 25 - 30.

[FN195]. *UECA*, *supra*, n. 28, s. 2(2)(6)

[FN196]. See New Brunswick Department of Justice, Law Reform Notes No. 15, September 2001.

[FN197]. *UECA*, *supra*, n. 28, s. 23; see discussion, *supra*, text at n. 130.

[FN198]. *New Brunswick Act*, *supra*, n. 150, s. 16(3).

[FN199]. *Ibid*., s. 10(2).

[FN200]. *UECA*, *supra*, n. 28, s. 1, set out *supra*, text at n. 81.

[FN201]. *New Brunswick Act*, *supra*, n. 150, s. 1(1).

[FN202]. Compare for example the definitions of “electronic” in the *UECA* and in the *New Brunswick Act*, or the consent provisions (*UECA* s. 6, *New Brunswick Act* s. 3), or the signature sections (s. 10 of each statute).

[FN203]. Almost all the implementing jurisdictions have put their own stamp on the *UECA*, however. The *Ontario Act* is probably the most radically restructured, without affecting the principles. The question is one of degree only, and is inherent in the nature of harmonized legislation in a federal state.

[FN204]. S.Q. 2001 c. 32, online at: *<http://publicationsduquebec.gouv.qc.ca/en/cgi/telecharge.cgi/161A0129.PDF?tableWgazette_pdf&docW66161A0129PDF&gazetteW664&fichierWWW161A0129.PDF>*.

[FN205]. As can been seen from the list of legislation *supra*, n. 150, some of the provincial implementations of the *Uniform Act* have removed the word “commerce” from its title, or added more to it, to reflect the broader scope.

[FN206]. *Quebec Act*, *supra*, n. 204, s. 1(2).

[FN207]. *Ibid*, s. 3.

[FN208]. *Ibid*, ss. 6 and 7.

[FN209]. See C. Reed, “What is a Signature?”, *supra*, n. 83.

[FN210]. See Don McGowan, “Quebec's Proposed Law on Information Technology Should Never See the Light of Day” in (2001), 1 Internet and E-Commerce Law in Canada 89, and a reply by Christine Carron, “Quebec's Proposed New Technologies Bill: Let the Light Shine In!”, (2000-01), 2 Internet and E-Commerce Law in Canada 1. The technology neutrality of the Quebec and *Uniform Act*s is discussed in J. D. Gregory, “Quebec's Proposed New Technology Bill: An Outside View” (2000-01), 2 Internet and E-Commerce Law in Canada 31.

[FN211]. The Act, formerly Bill C-6 (and before that Bill C-54) was given Royal Assent on April 13, 2000, as S.C. 2000 c. 5. See the Act online at: < *http://laws.justice.gc.ca/en/P-8.6/index.html*>.

[FN212]. The electronic evidence rules are discussed *infra* in the text accompanying n. 262.

[FN213]. The scope is different from that of Part 1 of *PIPEDA* on privacy, which over time expands to cover commercial activity in areas traditionally the subject of provincial jurisdiction.

[FN214]. *PIPEDA*, *supra*, n. 211, s. 33.

[FN215]. *UECA*, *supra*, n. 28, s. 2(5).

[FN216]. *PIPEDA supra*, n. 211, s. 34. Compare *UECA*, *supra*, n. 28, s.18.

[FN217]. *PIPEDA supra*, n. 211, s. 35. Compare *UECA*, *supra*, n. 28, s. 16.

[FN218]. *PIPEDA supra*, n. 211, s. 49.

[FN219]. *Ibid.*, s. 41.

[FN220]. *Ibid.*, s. 43.

[FN221]. *Ibid.*, s. 47.

[FN222]. *Ibid.*, s. 40.

[FN223]. *Ibid.*, s. 36.

[FN224]. *Ibid.*, s. 39.

[FN225]. *Ibid.*, s. 44 (which also requires designation and regulations as above).

[FN226]. *Ibid.*, s. 45.

[FN227]. *Ibid.*, s. 46.

[FN228]. *Ibid.*, s. 31.

[FN229]. Online at: <*http://www.nist.gov*>.

[FN230]. The California Digital Signature Regulations are online at: < *http://www.ss.ca.gov/digsig/regulations.htm*>.

[FN231]. *Illinois Electronic Commerce and Security Act*, 1998, s. 10-110, online at: <*http://*

www.legis.state.il.us/ilcs/ch5/ch5act175articles/ch5act175artstoc.htm>.

[FN232]. Notably Washington, Minnesota and Missouri. See the sources for electronic signature legislation, *supra*, n. 26.

[FN233]. *Supra*, n. 93.

[FN234]. *Supra*, n. 93.

[FN235]. *PIPEDA, supra*, n. 211, s. 48.

[FN236]. Cross-certification allows two or more public key infrastructures to recognize each other's certificates and thus signatures. More on the Government of Canada PKI can be found online at <*http://www.cio-dpi.gc.ca/pki-icp/index_e.asp*>. While secure electronic signatures will depend on the use of encryption, nothing in this article deals with the use of encryption to maintain confidentiality of documents. Confidentiality is not usually required of documents for them to have legal effect. It protects other interests.

[FN237]. *Supra*, n. 108.

[FN238]. R. Tassé & K. Lemieux, “Consumer Protection Rights in Canada in the Context of Electronic Commerce” online at: <*http:// strategis.ic.gc.ca/SSG/ca01031e.html*>.

[FN239]. The letter is online at: <*http://www.piac.ca/uecalet.htm*>.

[FN240]. The Guidelines are available at the Industry Canada e-commerce web site, online at: <*http://strategis.gc.ca/SSG/ca01182e.html*>.

[FN241]. Online at: <*http://www.safeshopping.org*>.

[FN242]. Online at: <*http://www.oecd.org/subject/e_commerce/*> and <*http:// www.oecd.org/dsti/sti/it/consumer/*>.

[FN243]. The principles are mentioned in the then Ministry of Consumer and Commercial Relations' consultation paper, Consumer Protection for the 21st Century (Ministry of Consumer and Commercial Relations, Toronto, 2000), at 8-9, online at: <*http://www.cbs.gov.on.ca/pdf/EnConsProt.pdf*>. The working group has made efforts to ensure that its proposals will be consistent with the *Uniform Electronic Commerce Act* and supplement rather than to displace it.

[FN244]. Part VI of the Manitoba statute, *supra*, n. 150, amended *The Consumer Protection Act*, C.C.S.M. c. C200.

[FN245]. Section 36 of the Manitoba statute created a new part of *The Consumer Protection Act*, ss. 127 - 135 of that Act, entitled “Internet Agreements”. The term “Internet” is defined in s. 127.

[FN246]. New s. 134 of *The Consumer Protection Act, supra*, n. 214.

[FN247]. Internet Agreements Regulation, Manitoba Regulation 176/2000, December 14, 2000.

[FN248]. See online at: <*http://www.ccr.gov.on.ca/pdf/EnConsProt.pdf*>. The April 2001 Throne Speech repeated the promise, though at time of writing no legislation had been introduced.

[FN249]. Internet Sales Contract Harmonization Template (2001), online at: < http://strategis.ic.gc.ca/SSG/ca01642e.html>

[FN250]. The Alberta draft was circulated among stakeholders but not published.

[FN251]. *New Brunswick Electronic Transactions Act*, *supra*, n. 150, gives power to make regulations "respecting consumer contracts or other consumer transactions that are entered into electronically, in whole or in part" (s. 19(1)(g)). No such regulation has yet been made, for Internet contracts or more broadly.

[FN252]. For example, *Alberta's Fair Trading Act*, R.S.A. 2000 c. F-2, makes provision for regulations to protect consumers in electronic commerce. Section 42 says that the Minister may make regulations respecting the marketing of goods and services through forms of electronic media, such as telephone, television or the Internet, that are specified in the regulations. In particular, regulations may be made regulating and prohibiting specific activities involved in electronic marketing, and to set out rights and remedies of consumers who enter into transactions wholly or partly through a form of electronic media. In May 2001, Alberta made its Internet Sales Contract Regulation, A.R.81/2001, to adopt the template, online at: *<http:// www.q.p.gov.ab.ca/documents/regs/2001_081.cfm>*.

[FN253]. See papers commissioned by the Consumer Measures Committee and by the Uniform Law Conference of Canada on court jurisdiction (private law) and regulatory jurisdiction (public law). *Supra*, n. 134. The American Bar Association published a major study of jurisdiction issues in 2000, online at: *<http://www.kentlaw.edu/cyberlaw>*.

[FN254]. *Supra*, n. 87. Proposed federal "interim final" rules pursuant to this Act have been published by the Federal Reserve Board for financial transactions. Online at: *<http:// www.federalreserve.gov/BoardDocs/Press/boardacts/2001/20010329/>*.

[FN255]. *E-SIGN*, *supra*, n. 87, s. 103(b)(2).

[FN256]. *Ibid.*, s. 101(c)(1)(C)(ii).

[FN257]. More discussion of this issue appears online at: *<http:// www.uetaonline.com>*.

[FN258]. Online at: *<http:// europa.eu.int/ISPO/ecommerce/legal/documents/31997L0007/31997L0007_en.html>*.

[FN259]. Online at: *<http:// europa.eu.int/ISPO/ecommerce/legal/documents/dissel/disselen.pdf>* (noting that the controversial amendment to Article 12 was withdrawn as contrary to the Brussels Convention on the Recognition and Enforcement of Judgments in Civil and Commercial Matters). See A. Salaün, "Consumer Protection Issues in Electronic Commerce Legal Issues" (2001), online at: *<http:// www.europa/eu.int/ISPO/legal/en/lab/991216/consumer_protection.doc>*.

[FN260]. Directive 98/27/EC on Injunctions for the Protection of Consumers' Interests.

[FN261]. Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market.

[FN262]. It is extremely rare for legislation in Canada to deal with the *weight* of evidence once it is before the court. That issue is left to the judges.

[FN263]. The only case that comes to mind is *R. v. Sheppard* (1992), 97 Nfld. & P.E.I.R. 144, [1992] N.J. No. 73, 1992 CarswellNfld 268, 308 A.P.R. 144 (Nfld. T.D.).

[FN264]. For an overview of the main issues, see Hamish Stewart, "Some Thoughts on Computer-Generated Evidence", [1996] Proceedings of the Uniform Law Conference of Canada 164, online at: <*http://www.ulcc.ca/en/poam2/index.cfm?secW1996&subWWW1996aa*>. A review of case law and former law reform efforts, together with proposals for change, is found in E. Tollefson, "Computer Produced Evidence in Proceedings within Federal Jurisdiction" in [1995] Proceedings of the Uniform Law Conference of Canada, online at: <*http:// www.ulcc.ca/en/poam2/index.cfm?secW1995&subW1995ad*, from para. 81>.

[FN265]. The leading text on evidence in Canada is Sopinka, Lederman, Bryant, *The Law of Evidence in Canada*, 2d ed. (Toronto: Butterworths, 1999). See also Alan M. Gahtan, *Electronic Evidence*, (Toronto: Carswell, 1999).

[FN266]. R.S.C. 1985 c. C-5.

[FN267]. R.S.C. 1985 c. C-46.

[FN268]. See for example the *Ontario Evidence Act*, R.S.O. 1990 c. E.23.

[FN269]. Civil Code of Quebec, Book VII.

[FN270]. See J. D. Ewart, Documentary Evidence in Canada, (Toronto: Carswell, 1984).

[FN271]. See for example *R. v. George* (1993), [1993] A.J. No. 798, 1993 CarswellAlta 170, 14 Alta. L.R. (3d) 106, 146 A.R. 107 (Alta. Prov. Ct.), paras 34, 60-64, where the court held that a computerized analysis of stock trading patterns was a form of expert evidence, so the analyst's qualifications as an expert witness needed to be proved.

[FN272]. Uniform Law Conference of Canada, Consultation Paper on Electronic Evidence, March 1997, online at: <*http://www.ulcc.ca/en/poam2/index.cfm?secW1997&subWWW1997aka*>.

[FN273]. [1998] Proceedings of the Uniform Law Conference of Canada 164, online at: <*http://www.ulcc.ca/en/us/index.cfm?secW1&subW1u2*>.

[FN274]. *Infra*, text at n. 299ff.

[FN275]. [1970] S.C.R. 608, 1970 CarswellAlta 80, 1970 CarswellAlta 142, 12 C.R.N.S. 349, 73 W.W.R. 347, 14 D.L.R. (3d) 4 (S.C.C.).

[FN276]. *Ontario Evidence Act*, *supra* n. 268, s. 35.

[FN277]. *Uniform Electronic Evidence Act*, *supra*, n. 273, s. 2.

[FN278]. See *R. v. Khan*, [1990] 2 S.C.R. 531, 1990 CarswellOnt 108, 1990 CarswellOnt 1001, [1990] S.C.J. No. 81, 113 N.R. 53, 79 C.R. (3d) 1, 41 O.A.C. 353, 59 C.C.C. (3d) 92 (S.C.C.); *R. v. Smith*, [1992] 2 S.C.R. 915, 1992 CarswellOnt 103, [1992] S.C.J. No. 74, 1992 CarswellOnt 997, 15 C.R. (4th) 133, 75 C.C.C. (3d) 257, 55 O.A.C. 321, 139 N.R. 323, 94 D.L.R. (4th) 590 (S.C.C.); *R. v. U. (F.J.)*, [1995] 3 S.C.R. 764, 1995 CarswellOnt 555, 1995 CarswellOnt 1175, 42 C.R. (4th) 133, 101 C.C.C. (3d) 97, 128 D.L.R. (4th) 121, 186 N.R. 365, 85 O.A.C. 321 (S.C.C.).

[FN279]. In the words of Wigmore on Evidence, cited in J. D. Ewart, Documentary Evidence in Canada, *supra* n. 270, at 13. Compare the language of the Civil Code of Quebec, noted *infra* n. 308.

[FN280]. See for example his opening contribution to the Uniform Law process, "Computer-produced Records in Court Proceedings", [1994] Proceedings of the Uniform Law Conference, online at: <*http://www.ulcc.ca/en/poam2/index.cfm?secW1994&subW1994ac*>.

[FN281]. (1978), 42 C.C.C. (2d) 67, 1978 CarswellOnt 58, 6 C.R. (3d) 218 (Ont. H.C.), affirmed (1979), 100 D.L.R. (3d) 671, 25 O.R. (2d) 301, 47 C.C.C. (2d) 499 (Ont.C.A.).

[FN282]. Ewart, Documentary Evidence in Canada, *supra* n. 270, at 67.

[FN283]. S. Schiff, *Evidence in the Litigation Process*, 3rd ed. (Toronto: Carswell, 1988) 728.

[FN284]. *Uniform Electronic Evidence Act*, *supra*, n. 273, s. 3.

[FN285]. *Ibid.*, annotation to s. 3.

[FN286]. *R. v. McMullen*, *supra* n. 281.

[FN287]. *R. v. Vanlerberghe* (1976), 6 C.R. (3d) 222, 1976 CarswellBC 61 (B.C. C.A.).

[FN288]. *Supra*, n. 25.

[FN289]. Though of course not for the purposes of the litigation, but for record-management reasons independent of the litigation.

[FN290]. *Uniform Electronic Evidence Act*, *supra*, n. 273, s. 4(1).

[FN291]. But Ontario amended the electronic records section of its *Evidence Act* in 2001 to add the possibility of demonstrating the reliability of an electronic record through the use of encryption. *Red Tape Reduction Act, 2000*, S.O. 2000 c. 26, Schedule A, section 7(1), proclaimed in force April 15, 2001. Alberta has adopted this change in its electronic evidence bill, which is part of its *Electronic Transactions Act*, *supra*, n. 150, s. 33.

[FN292]. This looks like a test that appeared in an English statute from the 1960s, the *Police and Criminal Evidence Act*, section 69. The *Uniform Act*'s language has been modified in light of later case law that dealt with the immaterial misfunction. *R. v. Shephard* [1993] A.C. 380, [1993] 1 All E.R. 225 (U.K. H.L.). The English test has been criticized as unnecessary, on the ground that the law already presumes that machines function as they are supposed to, unless the opposite is shown. A. Hoey, "Analysis of the Police and Criminal Evidence Act, section 69 - Computer Generated Evidence", [1996] 1 Web J.C.L.I., online at: <*http://www.ncl.ac.uk/~nlawwww/1996/issue1/hoey1.html*>, and Consultation Paper 138 of the Law Commission of England and Wales, 1995, paragraphs 14.27 to 14.32. It is far from clear that such a presumption operates in Canadian law, or if it does, that it would apply to computerized record systems. New types of machine generally have to be shown to work before the courts effectively, if not formally, shift the burden of proof about their reliability.

[FN293]. *Uniform Electronic Evidence Act*, *supra*, n. 273, s. 6.

[FN294]. CAN/CGSB-72.11-93.

[FN295]. The standard as amended to April 2000 can be ordered online from: <*http://www.pwgsc.gc.ca/cgsb/catalogue/specs/072/072_011-e.html*>.

[FN296]. *Uniform Electronic Evidence Act, supra*, n. 273, s. 1.

[FN297]. (1982), 65 C.C.C. (2d) 377, 1982 CarswellOnt 61, 35 O.R. (2d) 164, 26 C.R. (3d) 336(Ont. C.A.), affirmed 1985 CarswellOnt 954, (sub nom. *Bruce v. R.*) [1985] 2 S.C.R. 287, 55 O.R. (2d) 287n (S.C.C.).

[FN298]. The definition section of the federal *Personal Information Protection and Electronic Documents Act, supra* n. 211, seems to make this mistake: see section 31(1). This is appropriate for Part 3 of *PIPEDA* on evidence (now s. 31.8 of the *Canada Evidence Act, supra*, n. 266), but arguably not for Part 2 on electronic documents.

[FN299]. *Supra*, n. 211, first introduced as Bill C-54 in October, 1998.

[FN300]. *Ibid.*, s. 56, now s. 31.4 of the *Canada Evidence Act, supra*, n. 266. Secure electronic signatures are discussed *supra* in the text accompanying n. 223.

[FN301]. *Ontario Evidence Act, supra* n. 268, s. 34.1, enacted by the Red Tape Reduction Act, 1999, S.O. 1999 c. 12, Sched. B, s. 7(2). The section came into force on June 30, 2000.

[FN302]. *Supra*, n. 291.

[FN303]. *Saskatchewan Evidence Amendment Act*, 2000, S.S. 2000 c. 61, online at: <*http://www.qp.gov.sk.ca/documents/english/firstread/1999-2/bill-34>pdf*>, now part of *The Saskatchewan Evidence Act*, R.S.S. 1978 c. S-16.

[FN304]. *Supra*, n. 153.

[FN305]. *Electronic Evidence Act*, S.Y.2000 c. 11.

[FN306]. *Electronic Evidence Act*, S.P.E.I. 2001 c. 32, online: <*http:// www.gov.pe.ca/law/statutes/pdf/e-04_3.pdf*>.

[FN307]. *Supra*, n. 150, s. 33.

[FN308]. The Code is online at: <*http:// www.lexum.umontreal.ca/ccq/en/index.html*>.

[FN309]. S.N.B. 1996 c. 52.

[FN310]. As noted, privacy is not discussed in this article. Other potential areas of legislation not yet taken up in Canada, or much discussed, include cryptography, information licensing and public key infrastructure.
17 BFLR-CAN 277

17 B.F.L.R. 277

END OF DOCUMENT