PRB 00-12E

Library of Parliament / Bibliothèque du Parlement

THE DEVELOPMENT OF LAWS ON ELECTRONIC DOCUMENTS AND E-COMMERCE TRANSACTIONS

Alysia Davies
Legal and Legislative Affairs Division

Revised 20 December 2008

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

CONTENTS

Page

CANADA
LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

THE DEVELOPMENT OF LAWS ON ELECTRONIC DOCUMENTS AND E-COMMERCE TRANSACTIONS*

INTRODUCTION

Electronic commerce has had a dramatic impact on the way in which business is done. Increasingly, business communications are being conducted online, as businesses adapt their operations to an electronic environment. In a new business environment where electronic transactions have become the norm, the use of paper to document business transactions is becoming less important. In fact, one of the benefits of conducting business by using digitized information is that it obviates the need to transmit and store paper.

Although businesses are adapting to the electronic environment, legal rules continue to stipulate that certain transactions or documents be in writing. Many see such legal requirements as an impediment to transacting business electronically. It is argued that, with a few exceptions, there is little or no benefit in requiring that electronic transactions be put in written form and signed manually. Indeed, it is now widely recognized that legal requirements calling for written documents and manual signatures must somehow accommodate the world of electronic communications. This view has been the driving force behind efforts by international bodies and individual countries to develop rules which would give the same level of legal recognition to electronic transactions as is accorded to paper documents that perform the same function.

This paper will review the development of legislation governing the use of electronic alternatives to paper-based forms of communication by the United Nations and in the United States, Australia, the European Union and Canada.

---

* This is a revised version of *Facilitating Electronic Commerce through the Development of Laws to Recognize Electronic Documents and Transactions*, prepared by Margaret Smith, formerly of the Library of Parliament, on 20 November 2000.

UNITED NATIONS

To further its mandate to promote the harmonization and unification of international trade law, the United Nations Commission on International Trade Law (UNCITRAL) adopted two documents: the UNCITRAL Model Law on Electronic Commerce in 1996, and the UNCITRAL Model Law on Electronic Signatures in 2001. In addition, the United Nations as a whole body adopted the *Convention on the Use of Electronic Communications in International Contracts* in 2005.

A. UNCITRAL Model Law on Electronic Commerce

The UNCITRAL Model Law on Electronic Commerce was developed in response to the rapid changes that were taking place in the methods of communication used to conduct business and international trade. As the use of electronic mail and electronic data interchange increased and became more prevalent, the existence of legal impediments to electronic communications and uncertainty about their legal effect and validity became evident.

UNCITRAL's decision to formulate model legislation on electronic commerce was also a response to the fact that much of the existing legislation governing the communication and storage of information did not contemplate the use of electronic commerce. In a number of cases, the legislation in place imposed or implied restrictions on the use of modern means of communication, for example, by prescribing the use of "written," "signed" or "original" documents.(1)

The Model Law on Electronic Commerce aims to provide national legislatures with a set of internationally recognized rules to remove legal obstacles and create a more certain legal environment for electronic commerce. It seeks to provide equivalent treatment for users of paper-based documentation and for users of computer-based information. As a "framework" law, however, it does not set out all the rules or cover every aspect of the use of electronic commerce.

---

(1) United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996*, New York, 1999, para. 3, p. 16, http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

The Model Law on Electronic Commerce adopts a "functional equivalent approach" to dealing with electronic commerce. This approach is based on analyzing the purposes and functions of paper-based requirements and determining how those purposes and functions can be fulfilled through electronic-commerce techniques. For instance, paper documents serve some of the following functions:

- They provide a legible document.
- They ensure that a document remains unaltered.
- They allow for the reproduction of documents so that parties can have a copy of the same data.
- They allow for the authentication of data by means of a signature.
- They provide that a document will be in a form acceptable to public authorities and courts.(2)

The Guide to the Model Law on Electronic Commerce notes that for "all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met."(3)

Article 5 sets out the fundamental principle of the Model Law on Electronic Commerce: that electronic communications should not be discriminated against or denied legal effect simply because they are in electronic form. Article 6 establishes the basic standard to be met by an electronic document when there is a legal requirement for a document to be in writing; it provides that a legal requirement to present information in writing will be met by providing an electronic document if information contained in the document is "accessible so as to be usable for subsequent reference."

Article 7 of the Model Law on Electronic Commerce acknowledges that in a paper-based environment, the role of a signature is to indicate approval of a document's contents and to verify the document's authenticity. This article provides that a requirement for a person's signature will be met in the case of an electronic document if a reliable method is used to identify the person and to indicate the person's approval of the information contained in the document.

(2) Ibid., para. 16, p. 20.

(3) Ibid., pp. 20-21.

Because of the increased acceptance around the world of electronic means as a substitute for traditional authentication and the need for uniformity in the law on this point, UNCITRAL has since adopted an entire Model Law devoted to electronic signatures alone, which is outlined in the next subsection of this paper. It is based on the principle of flexibility established by Article 7.(4)

Another important function carried out by a paper-based document is to satisfy a legal requirement for an original document. Article 8 of the Model Law on Electronic Commerce aims to remove the obstacles that a requirement for an original document may pose to electronic documents. It provides that where the law requires information to be presented or retained in its original form, that requirement will be met by an electronic document if:

- there is a reliable assurance as to the integrity of the information from the time when it was first generated in its final form as an electronic document; and
- the information is capable of being displayed to the person to whom it is to be presented.

Article 9 of the Model Law on Electronic Commerce deals with the admissibility of electronic documents in legal proceedings.

Article 10 addresses the legal requirement for certain documents to be retained for a period of time or for specified purposes by setting out the conditions that must apply if electronic documents are to meet this requirement. These conditions include:

- being able to access the information contained in the electronic document so that it can be usable for subsequent reference;
- retaining the document in the format in which it was generated, sent or received; and
- retaining the information to enable the identification of the origin and destination of the document as well as the time when it was sent or received.

Another important purpose of the Model Law on Electronic Commerce is to inject certainty into contracts that are concluded electronically. The Model Law deals with the formation of contracts, the form in which an offer and acceptance may be expressed, and the time and place of dispatch and receipt of electronic documents. It does not, however, change the law dealing with the formation of contracts.

---

(4) United Nations Commission on International Trade Law, *2001 – UNCITRAL Model Law on Electronic Signatures with Guide to Enactment*, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.

In formulating the Model Law on Electronic Commerce, the UNCITRAL drafters believed that electronic communications would most likely be used for contracts relating to the carriage of goods. As a result, Articles 16 and 17 deal specifically with documents in this area.

Since its inception, the UNCITRAL Model Law on Electronic Commerce has gained increasing international acceptance as the model upon which a number of national laws are being based. It has informed electronic commerce statutes in a number of countries, including the United States, Australia, the European Union and Canada.

B. UNCITRAL Model Law on Electronic Signatures

The UNCITRAL Model Law on Electronic Signatures, adopted in 2001, was intended as a response to the increasing number of international trade transactions carried out by means of electronic communication. It aims to promote the ability to rely on electronic signatures as equivalent to handwritten ones.(5)

The Model Law on Electronic Signatures is, like its counterpart, not a convention, but merely a model law that countries may find useful to apply when formulating legislation in this area. It is designed to be applied where electronic signatures are used in the context of commercial activities, but not to override any rule of law intended to protect consumers.(6)

It defines an "electronic signature" as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."(7) The term "data message" is defined as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy."(8)

Article 4 of the Model Law on Electronic Signatures provides guidance for settling any matters not expressly dealt with by it based on its underlying principles. Article 5 allows for the provisions of the law to be varied by agreement.

---

(5) United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, New York, 2002, pp. vii–viii, http://www.uncitral.org/pdf/english/ texts/electcom/ml-elecsig-e.pdf.

(6) Ibid., Article 1.

(7) Ibid., Article 2(*a*).

(8) Ibid., Article 2(*c*).

Article 6 applies a contextual analysis to the validity of electronic signatures – where a signature is required, that requirement is met by the use of an electronic signature if it is "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in light of all the circumstances." (This includes any agreement made by those involved.)

The reliability of an electronic signature is gauged by a number of factors outlined in Article 6:

- the signature creation data are linked to the signatory and to no other person in the context within which they is used;
- the data to create it were linked to the signatory and no other person at the time of the signing;
- any alteration made to it after the time of the initial signing is detectable; and
- where the signature is intended to vouch for the integrity of particular information, any later change to that information is also detectable.

The determination of reliability is intended to be made in accordance with international standards and the rules of private international law.

Article 8 places some responsibilities on the signatory to safeguard his electronic means of providing a signature. The signatory is required to "exercise reasonable care" to prevent unauthorized use of his or her signature creation data, and, in the case of that data being compromised (or a "substantial" risk of possible compromise having been detected), to notify anyone who might be affected as quickly as possible by means of the certification service provider. Where a certificate is used to support the electronic signature, the signatory must exercise reasonable care to ensure the accuracy and completeness of all representations that are relevant to the certificate through its life cycle. The signatory is legally liable for any failure to live up to these responsibilities.(9)

Article 9 outlines the obligations of any certification service provider who provides services to support an electronic signature used for legal effect. The provider is required to:

(9) Ibid., Article 8.

- act in accordance with its stated policies and procedures;

- exercise reasonable care to ensure the accuracy and completeness of all representations it makes about the electronic signature throughout its life cycle (or that are included in the certificate);

- provide reasonably accessible means to enable a relying party to ascertain from the certificate the provider's identity, the signatory's control of the signature at the relevant time, and the fact that the signature creation data were valid at or before the time the certificate was issued;

- provide means for a signatory to give notice as required under Article 8 where those services are offered, and to ensure the availability of a timely revocation service;

- utilize "trustworthy" systems, procedures and human resources in performing its services; and

- provide reasonably accessible means to enable a relying party to ascertain where relevant:

    - the method used to identify the signatory;
    - any limitation on the purpose or value for which the signature creation data or certificate may be used;
    - the validity and integrity of the signature creation data;
    - any limitation on the scope of extent of liability stipulated by the certification service provider;
    - the likelihood that means exist for the signatory to give notice under Article 8;
    - the likelihood that a timely revocation service is offered.

The certification service provider is liable for any failure to live up to the requirements of Article 9.

Article 10 provides additional information about what constitutes "trustworthiness" in systems, procedures and human resources used by a certification service provider. The factors that must be taken into account are financial and human resources (including the existence of assets); the quality of hardware and software systems; procedures for processing certificates, applications for certificates and retention of records; the availability of information to signatories and potential relying parties; and the regularity and extent of an audit by an independent body. Also required is the existence of a declaration by the state, an accreditation body or the certification service provider assuring compliance with all of these requirements. Article 10 also allows for "any other relevant factor" to be considered in assessing whether a certification service provider has provided trustworthy service.

Article 11 regulates the behaviour of the party relying on the electronic signature. This party bears liability for any failure to take reasonable steps to verify the reliability of an electronic signature, or, where the signature is supported by a certificate, any failure to take reasonable steps to verify the validity, suspension or revocation of the certificate and to observe any limitation with respect to the certificate.

Finally, Article 12 deals with recognition of foreign certificates and electronic signatures. It prohibits geographic discrimination in recognizing electronic signatures, stating that "no regard" shall be given to either the location where the signature is created electronically or the location of the signatory in determining the validity of an electronic signature. It also establishes that certificates and electronic signatures issued within a particular country will have the same legal effect as those issued outside it where there is an equivalent level of reliability as measured by international standards. Parties may agree among themselves as to the level of reliability notwithstanding these provisions, provided they do so in accordance with applicable law.

C. UN Convention on the Use of Electronic Communications in International Contracts

Up to 2005, UNCITRAL had issued only model laws that could be voluntarily adopted by interested countries to help them with their legislative designs. However, work on the laws had gradually helped to develop a consensus about the basic principles that should govern electronic commerce across the spectrum, and the United Nations has now adopted a full binding convention on them – the *UN Convention on the Use of Electronic Communications in International Contracts*.(10)

Article 1 of the convention establishes some basic principles, including that neither the nationality of the parties nor the civil or commercial character of their transaction is relevant to a determination under the convention.

Article 2 limits the application of the convention to commercial contracts only, stating that it does not cover contracts concluded for personal, family or household purposes. The convention also does not apply to the following:

- transactions on a regulated exchange;

---

(10) General Assembly of the United Nations, *2005 – United Nations Convention on the Use of Electronic Communications in International Contracts*, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

- foreign exchange transactions;
- inter-bank payment systems or agreements;
- clearance and settlement systems relating to securities or financial assets/instruments;
- the transfer of security rights in sale, loan or holding of an agreement to repurchase securities, or other financial assets/instruments held with an intermediary;
- bills of exchange;
- promissory notes;
- consignment notes;
- bills of lading;
- warehouse receipts; and
- any transferable document or instrument that entitles the bearer or beneficiary to claim delivery of goods or payment of a sum of money.

Parties may explicitly exclude themselves or derogate from the application of the convention by mutual agreement.(11)

The convention is built upon the model laws to a large extent, and contains many clauses that are similar or identical. It also contains a definitions section which has some modified or updated definitions. Electronic communication is defined as "any communication that the parties make by means of data messages." The definition of "data message" is the same as in both model laws, except the wording has been streamlined and "magnetic" has been added to the list of means of transmission.(12)

A definition of "communication" has also been added, stating that the term refers to "any statement, declaration, demand, notice or request, including an offer and the acceptance

(11) *United Nations Convention on the Use of Electronic Communications in International Contracts*, Article 3, New York, 2007, http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.

(12) Ibid., Articles 4(*b*) and (*c*); *UNCITRAL Model Law on Electronic Signatures*, Article 2(*c*); *UNCITRAL Model Law on Electronic Commerce*, Article 2(*a*).

of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract."[13]

The convention also contains a new section on the location of parties, establishing a presumption that a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that there is no place of business at that location. If a party with multiple places of business has not specified one, then it will be assumed to be the one at the location with the closest relationship to the relevant contract. If a party is a natural person without a place of business, the party's location will be the habitual residence.[14]

In addition, the convention attempts to address the issue of fraudulent business addresses by establishing that a location does not qualify as a place of business merely because it is where equipment and technology supporting information used by a party to the contract are located, nor does it qualify merely because parties may access an information system there. The fact that a party makes use of a domain name or electronic mail address connected to a specific country is also not enough to create a presumption that the party's place of business is located in that country.[15]

The convention provides rules to determine the time and place of electronic communications for the purposes of establishing a contract. An electronic communication is considered sent by a party once it leaves the information system under the party's control, unless it is being communicated internally within an information system, at which point it is considered sent once it arrives at the receiving party. The receipt of an electronic communication is defined as being the time when it becomes capable of being retrieved by the addressee at that party's electronic address, and the addressee becomes aware that it can be retrieved. Electronic communications are deemed to be sent to and received at the parties' places of business, notwithstanding the fact that the electronic address may be located in a place that differs from the place of business.[16]

General unaddressed electronic communications inviting multiple parties to make an offer and automatic message systems for contract formation are both deemed valid under the

---

(13) *United Nations Convention on the Use of Electronic Communications in International Contracts*, Article 4(*a*).

(14) Ibid., Articles 6(1)–6(4).

(15) Ibid., Articles 6(4) and 6(5).

(16) Ibid., Article 10.

convention, except when any local laws apply requiring parties to individually negotiate some or all of the terms of a contract. Where a person makes an error in an automated electronic communications system related to contract formation, that person is permitted to withdraw the error provided the other party is notified of it as soon as possible, and provided the party in error has not already used or received any material benefit from the exchange of goods and services with the other party.(17)

The convention was open for signature until 16 January 2008, at which point it had been signed by only 18 member countries.(18) However, it has also been endorsed by the International Chamber of Commerce.(19) It remains open indefinitely for ratification and accession.(20)

UNITED STATES

A. State Initiatives

In 1999, the National Conference of Commissioners on Uniform State Laws (NCCUSL) promulgated the *Uniform Electronic Transactions Act* (UETA). The UETA represents the first national effort to provide uniform rules to govern electronic commerce transactions.(21)

The UETA applies only to transactions that the parties have agreed to conduct electronically. It does not create a new system of legal rules for the electronic marketplace, but rather ensures that electronic transactions are equivalent to and as enforceable as paper-based transactions.

The basic rules, set out in section 7 of the UETA, provide that:

---

(17) Ibid., Articles 11, 12, 13 and 14.

(18) These countries are the Central African Republic, China, Colombia, Honduras, Iran, Lebanon, Madagascar, Montenegro, Panama, Paraguay, Philippines, Republic of Korea, the Russian Federation, Saudi Arabia, Senegal, Sierra Leone, Singapore and Sri Lanka.

(19) International Chamber of Commerce, "Business endorses UN convention on electronic contracting," News release, 19 June 2006, Paris, http://www.iccwbo.org/policy/ebitt/icchgdi/index.html.

(20) United Nations Information Service, "Honduras signs the United Nations Convention on the Use of Electronic Communications in International Contracts," News release, 17 January 2008, Vienna, http://www.unis.unvienna.org/unis/pressrels/2008/unisl116.html.

(21) National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act (1999)*, http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

- a record or signature may not be denied legal effect or enforceability solely because it is in electronic form;
- a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation;
- any law that requires writing will be satisfied by an electronic record; and
- any signature requirement in the law will be met if there is an electronic signature.

Most of the other rules in the UETA are derived from these basic rules and serve to answer legal questions about the use of electronic documents and signatures. Section 15, for instance, sets out when information is legally sent or delivered in electronic form. It establishes when electronic delivery takes place, that is, when an electronic record capable of retention by the recipient is legally sent and received.

The UETA defines and validates electronic signatures. An electronic signature is defined as "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record." It removes writing and signature requirements that create barriers to electronic transactions. The UETA ensures that contracts and transactions are not denied enforcement because electronic media are used.

Another rule supporting the validity of electronic documents and signatures in transactions is set out in section 9 of the UETA, which provides that a signature is attributable to a person if it is an act of that person, and that act may be shown in any manner. Section 10 establishes rules relating to errors and changes in electronic documents.

The UETA validates contracts formed by electronic agents, i.e., computer programs that operate automatically to conduct business in electronic form. It also protects against errors by providing appropriate standards for the use of technology to ensure the identification of the parties involved.

The UETA authorizes state governmental entities to create, communicate, receive and store records electronically, and encourages state governmental entities to move to electronic media. It also ensures that the courts accept electronic records into evidence.

To date, 46 American states have adopted some variation of the UETA. The four states which have not – Georgia, Illinois, New York and Washington – have enacted their own electronic signature statutes instead.(22)

B. Federal Initiatives

The US federal *Electronic Signatures in Global and National Commerce Act*(23) ("E-SIGN") was enacted by the federal Congress and came into effect on 1 October 2000. The Act gives electronic signatures and documents equivalent legal status with handwritten signatures and paper-based documents. It is technology-neutral so that the parties entering into electronic contracts can choose the system they want to use to validate an online agreement.

The law provides that no one is required to use or accept electronic documents or signatures. If a notice must be provided to a consumer in writing, an electronic version will meet that requirement only if the consumer consents to accepting an electronic version and can access the information in electronic form.

The Act specifies that a state can pre-empt the federal law, but only by adopting the *Uniform Electronic Transactions Act* or by passing a law that is consistent with the federal Act and essentially technologically neutral. In addition, the Act does not apply to documents such as:

- wills, codicils and testamentary trusts;
- adoptions, divorce or other family law matters;
- a notice of cancellation or termination of utility services or the default, acceleration, repossession, foreclosure or eviction under a credit agreement secured by, or a rental agreement for, an individual's primary residence;
- the cancellation or termination of health or life insurance benefits; or
- the recall or notification of a material failure of a product.

---

(22) National Conference of State Legislatures, "Uniform Electronic Transactions Act," http://www.ncsl.org/programs/lis/CIP/ueta-statutes.htm.

(23) United States, *Electronic Signatures in Global and National Commerce Act*, 2000, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761enr.txt.pdf.

Although many states have passed electronic signature laws, the US Congress held the view that a federal law was necessary because state electronic signature and electronic commerce statutes lacked uniformity. Some states, for example, provide that any type of electronic signature is valid. Others require some form of security such as tying the electronic signature to the person signing or being able to determine that the electronic message has not been altered. Still others recognize only digital signatures. In addition, state laws have provided different uses for electronic signatures. Some laws allow electronic signatures to be used only in relation to transactions with government agencies; others allow the signatures to be used only for certain kinds of commercial transactions.

AUSTRALIA

In 1999, the Australian Parliament passed the *Electronic Transactions Act 1999* (ETA).(24) The ETA is designed to facilitate the development of electronic commerce in Australia by removing existing legal impediments, under national law, to using electronic communications.

The Act is based on the recommendation of the Australian Electronic Commerce Expert Group that Australia enact legislation based on the UNCITRAL Model Law on Electronic Commerce.(25)

The ETA is founded on two principles:

- *functional equivalence* (sometimes called media neutrality): ensures that paper-based transactions and electronic transactions are treated equally by the law; and
- *technology neutrality*: ensures that the law does not discriminate between different forms of technology.

---

(24) Australia, *Electronic Transactions Act 1999*, No. 162, 1999, http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/11866D05A55BE8F6CA25730200002C72?OpenDocument.

(25) Information about the *Electronic Transactions Act 1999* is largely drawn from the following document: The Parliament of the Commonwealth of Australia, House of Representatives, *Electronic Transactions Bill 1999 – Explanatory Memorandum*, http://www.comlaw.gov.au/ComLaw/Legislation/Bills1.nsf/framelodgmentattachments/11303D1EFBAAC11CCA256F72002E0435.

The basic requirement under the Act for any electronic communication is that it be readily accessible so as to be usable for subsequent reference. This ensures that others will be able to access and use the information contained in the electronic communication. In addition, a person should also be able to retain the information in some way if he or she wishes to do so.

One of the basic requirements of the Act is that a person must consent to receiving electronic communications. Consent, however, can be either expressed or inferred from a person's conduct.

The Act sets out general rules that allow certain legal requirements to be satisfied by electronic communications. In addition to these general rules, the Act covers specific issues, such as electronic signatures. To comply with the Act, electronic signatures must identify the sender and indicate that party's approval of the information communicated. The Act provides for the production of an electronic document where the law requires the production of a paper document.

Other provisions deal with the electronic recording of information, the electronic retention of documents, and retention of electronic communications. The Act also sets out rules in relation to the time and place of sending and receiving electronic communications.

The ETA had a two-stage implementation process. As of 15 March 2000, the Act applied to certain laws specified in the *Electronic Transactions Regulations 2000*.(26) As of 1 July 2001, the Act applied to all national laws with a few exceptions, and the *Regulations* were altered to reflect the exceptions instead.(27) These exceptions include quite a considerable list of laws in the areas of Aboriginal land rights documents, aerospace sales, care agreements for the elderly, conservation, defence and certain research and development and financial transactions, among others.(28)

Along with developments at the national level, the national, state and territory governments together developed the Uniform Electronic Transactions Bill 2000, which the Attorney General announced had been enacted by all state and territory governments on 3 April 2000. The bill is closely modelled on the *Electronic Transactions Act 1999* and applies

---

(26) Australia, *Electronic Transactions Regulations 2000*, S.R. 2000, No. 19, http://www.comlaw.gov.au/comlaw/Legislation/LegislativeInstrument1.nsf/0/3D47793EC62C14C4CA256F700080CE5C?OpenDocument.

(27) Australian Government, Attorney-General's Department, "Australia's legal framework on electronic commerce," [Australian Attorney-General], rev. 10 September 2008, http://www.ag.gov.au/www/agd/agd.nsf/Page/e-commerce_Australiaslegalframeworkforelectroniccommerce.

(28) *Electronic Transactions Regulations 2000*.

to contract law, as well as to all dealings of the public with state and territory governments. Now each state and territory has its own Electronic Transactions Act, which generally mirrors the federal law except for some small modifications and additions in each instance.(29)

EUROPEAN UNION

On 4 May 2000, the European Parliament approved the Directive on Electronic Commerce.(30) Member states were to be required to implement the directive within 18 months by amending laws that could impede the use of electronic contracts. The directive provides that, in certain circumstances, member states will be able to maintain restrictions on the use of electronic contracts. It also obliges member states to impose requirements for the conclusion of electronic commerce to assist consumers in avoiding technical errors.(31)

By 2003, 12 member states had implemented the directive, although three – France, the Netherlands and Portugal – took a little longer.(32) As of 2008, all 27 members of the European Union (EU) have integrated some form of the directive into their national laws.(33) Two countries applying for EU membership, Turkey and Croatia, are also working towards adopting the directive, and the three affiliate countries that have signed the European Economic Area agreement – Iceland, Norway and Liechtenstein – have also implemented laws based on the directive.(34)

---

(29) Australian Attorney-General (2008).

(30) European Union, "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')," *Official Journal L 178*, 17.7.2000, p. 1-16, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT.

(31) European Union, "Electronic Commerce: Commission welcomes final adoption of legal framework Directive," News release, Brussels, 4 May 2000, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/00/442&format=HTML&aged=1&language=EN&guiLanguage=en.

(32) European Union, "e-commerce: EU law boosting emerging sector," News release, Brussels, 21 November 2003, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/1580&format=HTML&aged=1&language=EN&guiLanguage=en.

(33) European Union, "National Provisions Communicated by the Member States concerning Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')," Eur-Lex 72000L0031, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72000L0031:EN:NOT#FIELD_FR.

(34) Jos Dumortier, *Legal Study on Legal and Administrative Practices Regarding the Validity and Mutual Recognition of Electronic Documents with a View to Identifying the Existing Legal Barriers for Enterprises*, European Commission, European Union Tender No. ENTR/04/67,

The EU also promulgated two additional directives, the e-Signatures Directive in 1999[35] and the e-Invoicing Directive in December 2001,[36] which were adopted by all of the member countries. However, the e-Invoicing Directive, which was focused primarily on the processing of value-added tax (VAT) transactions, has now been integrated into a larger and more general new VAT Directive,[37] with which not all member countries have fully complied.[38]

The EU recently published the final report of an informal European Commission task force on e-invoicing, which recommends a new pan-European framework strategy for harmonizing e-invoicing practices. The EU is also working towards model standards to facilitate additional harmonization.[39]

CANADA

A. *Uniform Electronic Commerce Act*

In June 1999, the Uniform Law Conference of Canada adopted the *Uniform Electronic Commerce Act* (UECA), a model law designed to implement the principles of the UNCITRAL Model Law on Electronic Commerce.[40] Drafted over a two-year period, the

---

November 2006, http://ec.europa.eu/ enterprise/ict/policy/legal/2006-bm-cr/dumortier-final-report-draft.pdf, p. 14.

(35) European Union, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures" [the "e-Signatures Directive"], *Official Journal L 013*, 19/01/2000, P. 0012 – 0020, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML.

(36) European Union, "Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax" [the "e-Invoicing Directive"], *Official Journal L 15*, 17.1.2002, P. 24-28, [No longer in force] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0115:en:NOT.

(37) European Union, "Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax" [the "VAT Directive"], *Official Journal L 347*, 11/12/2006, P. 0001-0118, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:347:0001:01:EN:HTML.

(38) For example, the European Commission is currently pursuing measures against Poland, which has not yet brought its law into force with the new Directive. (See European Union, "VAT – Commission takes steps against Poland with regard to the application of rules on place of supply of services," News release, Brussels, 28 February 2008, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/335&format=HTML&aged=0&language=EN&guiLanguage=en.)

(39) European Commission Informal Task Force on e-Invoicing, *European Electronic Invoicing Final Report*, v. 3.2 (Final), EEI-3.2, July 2007, http://ec.europa.eu/enterprise/ict/policy/legal/index.htm.

(40) Uniform Law Conference of Canada, Uniform Electronic Commerce Act [UECA], August 1999, http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1.

UECA has been proposed as the model upon which provincial and territorial governments can develop a harmonized approach to electronic commerce.

The UECA is divided into three parts:

- Part 1 (sections 5–18) sets out rules for functional equivalence between electronic and paper-based documents, and spells out that they apply when the parties involved in a transaction have agreed, expressly or by implication, to use electronic documents. This part also allows governments to set their own rules for accepting electronic documents, because a blanket acceptance of any electronic communication may expose governments to formats and media that they cannot handle and that may not work for their particular purposes.

- Part 2 (sections 19–23) sets out rules for specific types of communications, such as the formation and operation of contracts, the effect of using automated transactions, the correction of errors when dealing with computer-based transactions, and deemed or presumed time and place of sending and receiving computer messages.

- Part 3 (sections 24–25) deals with the carriage of goods.

In Part 1, the governing principle of the UECA is set out in section 5, which provides that information shall not be denied legal effect or enforceability solely because it is in electronic form. Section 6 makes it clear that a person is not compelled to use electronic documents but a person's consent to do so may be inferred from the person's behaviour. For instance, providing one's e-mail address could be considered as consent to receive communications via e-mail. Information received by government, however, is subject to special provisions.

Under the UECA, a legal requirement that information be in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference.(41) A legal requirement for a person to provide information in writing to another person is satisfied by the provision of the information in an electronic document, if the electronic document is accessible by the other person and capable of being retained by that person so as to be usable for subsequent reference.(42) The drafters of the UECA reasoned that when the law requires someone to provide information to someone else in writing, then more is needed than mere accessibility. The recipient has to receive the document in a way that gives him or her control over what becomes of it. This section therefore requires the information to be accessible

(41) UECA, s. 7.

(42) UECA, s. 8.

for subsequent use, and that the information be capable of being retained by the person to whom it is provided.(43)

The UECA deals with legal requirements to provide information in a specific non-electronic form by allowing such information to be provided electronically if it is provided in the same or substantially the same form, and the electronic document is accessible by the other person and capable of being retained by the other person so as to be usable for subsequent reference.(44)

The UECA allows for the use of electronic signatures. The Act requires that the information purporting to constitute the signature be created or adopted by a person with the intent to sign the document, and that it be associated in some way with the document.(45) Signatures submitted to governments, however, would have to meet information technology standards and rules established by such governments.

Under section 11 of the UECA, an electronic document can function as an original if there are sufficient assurances about the integrity of the information in it.

Part 2 of the UECA covers the formation of contracts by electronic means. The Act does not change the general law of contracts, but rather seeks to ensure that electronic communications are capable of conveying the kinds of intention that are necessary to support contractual relations. Section 21 provides that a contract may be formed by the interaction of a computer and an individual or by the interaction of two computers. Section 22 deals with errors that may arise in these situations. The UECA provides that an electronic contract made by an individual with an electronic agent (computer) has no “legal effect and is not enforceable” if the individual made a material error in the document and

- the electronic agent did not provide the natural person with an opportunity to prevent or correct the error;

- the natural person notifies the other person of the error as soon as practicable when the natural person learns of it and indicates that he or she made an error in the electronic document;

- the natural person takes reasonable steps, including steps that conform to the other person’s instructions to return the consideration received, if any, as a result of the error or, if instructed to do so, to destroy the consideration; and

(43) UECA, s. 7.

(44) UECA, s. 9.

(45) UECA, s. 1.

- the natural person has not used or received any material benefit or value from the consideration, if any, received from the other person.

The UECA also establishes rules with respect to the time and place of sending and receiving electronic documents. Section 23 provides that a message is sent when it leaves the control of the sender and creates a presumption as to when a message is received. If the recipient designates an information system or uses a particular information system for receiving documents, then the document is presumed to have been received when it enters the information system. If the recipient does not designate or use an address, then the message is not presumed to be received until the addressee has notice of it, and is able to retrieve and process it.

Part 3, sections 24 and 25, of the UECA address the electronic versions of contracts pertaining to the carriage of goods.

B. Federal Initiatives

At the federal level, the *Personal Information Protection and Electronic Documents Act*(46) (PIPEDA) implements measures to create functional equivalency between electronic and paper documents. (It does not apply to contracts more generally, which are regulated under provincial jurisdiction.) Part 2 of PIPEDA provides for "the use of electronic alternatives … where federal laws contemplate the use of paper to record or communicate information or transactions."(47) Among other things, PIPEDA provides for:

- making payments to the federal government in electronic form;(48)
- submitting information to the federal government in electronic form;(49)
- using electronic documents to satisfy a requirement under federal law for a document to be in writing;(50)
- using electronic signatures; and(51)

(46) *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5.

(47) Ibid., s. 32.

(48) Ibid., s. 34.

(49) Ibid., s. 35.

(50) Ibid., s. 41.

(51) Ibid., s. 43.

- providing electronic documents when an original document is required.(52)

In some situations, PIPEDA requires the use of a "secure electronic signature" – an electronic signature resulting from the application of a prescribed technology or process.(53) Before a technology or process can be prescribed, it must be proved that:

- the electronic signature is unique to the person using it;
- the person whose electronic signature is on the document has control of the use of the technology to attach the signature;
- the technology can be used to identify the person using the electronic signature; and
- the electronic signature can be linked to an electronic document to determine if the document has been changed after the electronic signature was attached to it.(54)

The term "secure electronic signature" is given a more precise technical meaning in the federal *Secure Electronic Signature Regulations*, which came into effect in 2005. To meet the definition, a digital signature must result from the following consecutive sequence of operations:

- the application of a mathematical code, called a "hash function," that converts electronic data into a message digest format which will indicate whether the data have been altered;
- the application to the message digest of a private key, i.e., a form of encryption unique to the owner of a digital certificate;
- the incorporation of this encrypted message digest into the electronic document, in one form or another;
- the transmission of the electronic document and the encrypted message digest together with a digital signature certificate or the means of access to one;
- the application of a public key, i.e., a decryption device for a specific private key, contained in the digital signature certificate, to decrypt the encrypted message digest;
- the application of the earlier hash function to the data in the electronic document to generate a new message digest;
- verification that the first and second message digests are identical (and therefore that the data has not been intercepted in transit); and

(52) Ibid., s. 42.

(53) Ibid., s. 31.

(54) Ibid., s. 48(2).

- verification that the digital signature certificate is valid according to criteria laid out in the regulations.(55)

The regulations go on to stipulate that a digital certificate is valid only if, at the time it is used to digitally sign an electronic document using the steps outlined above, it is readable and perceivable by those allowed access to the digital signature certificate, and if it has not expired or been revoked. Any supporting certificates for the main digital certificate must also meet the same criteria.(56)

Certification authorities for these digital certificates are valid only if they are approved on a public list provided by the Treasury Board. As of the date of this paper, the only entities approved to issue digital certificates on the federal list are Public Works and Government Services Canada and the Canada Revenue Agency.(57)

PIPEDA also deals with electronic documents used as evidence in some legal proceedings. In a typical court proceeding, original documents are usually required to satisfy a court that the terms and conditions of an agreement have not been changed since the agreement was signed. This requirement is difficult to satisfy where electronic documents are involved because the original cannot be distinguished from an amended document and because handwritten signatures do not authenticate the document. PIPEDA requires the use of secure electronic signatures for electronic documents in certain instances, when the law provides for original documents or statements of truth.(58)

The handling of electronic evidence has evolved into a separate area of the law with its own statutory framework. A detailed *Uniform Electronic Evidence Act*, promulgated by the Uniform Law Conference of Canada in 1998, has been the basis for further amendments to the *Canada Evidence Act* and to the provincial evidence acts in Alberta, Saskatchewan, Manitoba, Ontario, Nova Scotia, New Brunswick, Prince Edward Island, Nunavut, and Yukon. The evidentiary rules in the *Quebec Civil Code* have also been amended.(59)

In addition, a set of model principles intended to be used by courts across the country as guidelines for e-discovery, called the *Sedona Canada Principles Addressing*

---

(55) *Secure Electronic Signature Regulations*, SOR/2005-30, s. 2.

(56) Ibid., s. 3.

(57) The list is posted at Treasury Board of Canada Secretariat, "Recognized Certification Authorities," http://www.tbs-sct.gc.ca/pki-icp/sesrca-sesac/sesr-sesa-eng.asp.

(58) PIPEDA, ss. 42, 44, 45 and 46.

(59) Bradley J. Freedman and Douglas G. Copland, eds., *Consolidated Electronic Commerce Statutes and Regulations With Related Materials 2008*, Thomson Carswell, Toronto, 2008, p. 306.

Electronic Discovery, were completed in early 2008.(60) The American predecessor to these principles had already been the subject of comment and application by Canadian judges before the Canadian version was completed,(61) and the courts are working on incorporating the principles into their official rules. The introduction of e-discovery is expected to greatly increase the price and complexity of litigation for businesses, governments, and other individuals and groups, introducing extra costs that could run as high as $1 million in certain types of cases.(62) This may drive a greater number of these cases towards settlement, at least until electronic document management systems that would simplify the e-discovery process are more widely adopted.

C. Provincial Initiatives

Provincial governments are moving to facilitate electronic commerce by clarifying the status of electronic documents and contracts. All of the provinces and territories, except for the Northwest Territories, have passed legislation to facilitate e-commerce and recognize electronic signatures and documents. Most of this legislation is based on the *Uniform Electronic Commerce Act*,(63) with the exception of Quebec's, which is a much broader and more comprehensive framework governing the application of information technology to documentation in general. While Quebec's legislation does incorporate many key elements of the *Uniform Electronic Commerce Act*, it is not technology neutral – it provides detailed prescriptions for what it deems the appropriate application of the technologies.(64)

---

(60) See The Sedona Conference, *The Sedona Canada Principles: Addressing Electronic Discovery*, January 2008, http://www.thesedonaconference.org/dltForm?did=canada_pincpls_FINAL_108.pdf.

(61) See, for example, *Air Canada* v. *Westjet Airlines Ltd.*, (2006), 81 O.R. (3d) 48; *Spielo Manufacturing and Manship* v. *Doucet and Dauphinee*, (2007), 327 N.B.R. (2d) 1; and *Spar Aerospace Limited* v. *Aeroworks Engineering Inc.*, (2007), [2008] 428 A.R. 84.

(62) Grant Buckler, "Evidence Mounts for Use of e-Discovery in Legal System," *The Globe and Mail*, 2 February 2004.

(63) The legislation in each province and Yukon and Nunavut is as follows: British Columbia: *Electronic Transactions Act*, SBC 2001, Ch. 10; Alberta: *Electronic Transactions Act*, S.A. 2001, c. E-5.5; Saskatchewan: *Electronic Information and Documents Act, 2000*, S.S. 2000, c. E-7.22; Manitoba: *Electronic Commerce and Information Act*, C.C.S.M., c. E55; Ontario: *Electronic Commerce Act, 2000*, S.O. 2000, c. 17; Quebec: *An Act to establish a legal framework for information technology*, R.S.Q., C-1.1; Nova Scotia: *Electronic Commerce Act*, S.N.S. 2000, c. 26; New Brunswick: *Electronic Transactions Act*, S.N.B. 2001, c. E-5.5; Prince Edward Island: *Electronic Commerce Act*, S.P.E.I. 2001, c. 31; Newfoundland and Labrador: *Electronic Commerce Act*, S.N.L. 2001, c. E-5.2; Yukon: *Electronic Commerce Act*, R.S.Y. 2002, Ch. 66; Nunavut: *Electronic Commerce Act*, S.Nu. 2004, c. 7.

(64) Freedman and Copland (2008), pp. 30–31.

The other provincial and territorial Acts conform more closely to the *Uniform Law on Electronic Commerce*, and contain the same exceptions – their electronic documents legislation does not apply to wills, bequest trusts, most powers of attorney, land transfer or registry records, and negotiable instruments including documents of title. All of these documents either do not retain legal force if conducted electronically, or are governed by separate legislation restricting the role of electronic communications.

However, some provinces and territories have aspects that differ from the overall framework. For example, Alberta's *Electronic Transactions Act* also explicitly does not apply to personal directives, guarantees or to land records involving rights to mines and minerals.(65) An additional regulation in effect until 2012(66) exempts records of employment and other records related to the employer–employee relationship, as well as certain types of health records and property records, and the records of some courts. Some of them will clearly come under the main regime within a few years, however.

Saskatchewan additionally excludes documents created under its *Health Care Directives and Health Care Substitute Decision Makers Act*(67) and those related to summary offences.(68) New Brunswick has promulgated a regulation specifically excluding from its electronic documents legislation seven acts in such areas as income security, family services, health records, adoption, and housing programs.(69)

Some provinces have expanded the use of electronic documents further than even suggested by the model law. Manitoba's *Electronic Commerce and Information Act* does not contain a provision explicitly excluding wills, bequest trusts, powers of attorney, or land registry and transfer documents, so it appears these transactions can be conducted electronically if the security requirements are met. Similarly, PEI's legislation does not include land registry and transfer documents.

Manitoba has not yet proclaimed the parts of its legislation that allow documents required under provincial laws to be replaced by electronic equivalents.(70) However, it has launched an e-government initiative by introducing a *Common Business Identifiers Regulation* that assigns a "common business identifier" – i.e., a unique alphanumeric identifier for a

(65) *Electronic Transactions Act*, S.A. 2001, c. E-5.5, s. 7.

(66) *Electronic Transactions Act General Regulation (Alberta)*, Alta. Reg. 34/2003.

(67) *Electronic Information and Documents Act, 2000*, S.S. 2000, c. E-7.22, s. 4(1)(*b*).

(68) *The Electronic Information and Documents Regulations (Saskatchewan)*, R.R.S., c. E-7.22, Reg. 1.

(69) *Exclusion Regulation – Electronic Transactions Act (New Brunswick)*, N.B. Reg. 2002-24.

program account with a public body – to all registered businesses in the province that interact with the government at any point.(71)

Legislation that is based on the *Uniform Electronic Commerce Act* contains a series of "functional equivalency" rules which set out the conditions that must be met for an electronic communication to satisfy a legal requirement for written communication. For example, when information or a document must be in writing, the electronic equivalent is acceptable if it is accessible so as to be usable for subsequent reference. Where there is a legal requirement to provide information or a document to a person in writing, an electronic document will satisfy the requirement if it is accessible and capable of being retained by the person to whom it is provided.

All provincial legislation establishes that an electronic document will be equivalent to an original document. Where there is a legal requirement for an original document to be provided, retained or examined, an electronic document will be acceptable if the integrity of the information has been maintained. In addition, electronic signatures will satisfy a legal requirement for a written signature.

The retention of documents and provision of copies are also covered. Where a document has to be retained for a period of time, an electronic version can be retained if it is accurate and available to the same extent as the original document and for the same length of time. Where multiple copies of a document must be provided, a single electronic version is acceptable.

Rules are established for the formation of contracts by electronic means which:

- allow a contract to be formed by using electronic communication which includes an action such as touching or clicking on an icon or place on a computer screen;
- allow a valid contract to be made by way of electronic communication that is automated at one or both ends of the transaction;
- permit a transaction entered into between an individual and an electronic agent (computer program) to be cancelled if a significant mistake is made, if there is no opportunity to prevent or correct the mistake, and the individual does not benefit from the transaction; and
- determine when messages are sent electronically, and when they are presumed to have been received.

---

(70) *Electronic Commerce and Information Act*, C.C.S.M., c. E55, Part 2.

(71) *Common Business Identifiers Regulations (Manitoba)*, Man. Reg. 176/2002.

These legislative provisions aim to provide increased legal certainty to the formation of contracts in an online environment.

Following upon the *Uniform Electronic Commerce Act*, the legislation also provides for the formation of contracts for the carriage of goods by electronic means.

It is important to note that most of the provincial legislation does not specify what an electronic signature is, other than to provide a general definition along the following lines: information in electronic form that a person creates or adopts in order to sign a document and that is attached to or associated with the document. An electronic signature therefore could be a digitized image of a handwritten signature, a biometric signature such as an electronically recorded thumbprint, a person's name spelled in ASCII characters, a digital signature using a public key infrastructure and a certification authority, or a voiceprint of a person saying his or her name. Only Ontario has specified in its legislation that biometric signatures are excluded – it appears they will be governed by separate legislation.(72)

However, the power to select certain technologies or define standards for them is contained in most of the legislation, so other jurisdictions may start to regulate the choice of technologies more closely in the future. The federal *Secure Electronic Signature Regulations* are the only ones of this type so far. Industry Canada has also released the *Principles for Electronic Authentication – A Canadian Framework*, a document to be updated every five years, which outlines the principles that should guide the development of technical standards. It was developed with the extensive input of standards groups, industry, and several provinces.(73)

Quebec's more extensive legislative framework goes into some detail about certificates and biometrics and establishes a harmonization committee to create technical standards for Quebec.(74) The legislation also refers to any standards established by the Standards Council of Canada and the International Organization for Standardization as legitimate for the purposes of fulfilling security and reliability requirements under the legislation.(75)

Finally, it is important to note that none of the provincial legislation compels a person to provide, use or retain documents in electronic form; however, a person's consent to do so can be inferred from the person's conduct.

D. Other Related Legislative Initiatives

(72) *Electronic Commerce Act, 2000*, S.O. 2000, c. 17, s. 29.

(73) Industry Canada, *Principles for Electronic Authentication: A Canadian Framework*, May 2004, http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html.

(74) *An Act to establish a legal framework for information technology*, R.S.Q., c. C-1.1, ss. 63–67.

(75) Ibid., s. 68.

As e-commerce develops into a more sophisticated and everyday form of commercial interaction, many other areas it touches are becoming increasingly regulated. The new cybermarket has coincided with the introduction of consumer protection Acts in Ontario(76) and British Columbia(77) and new regulations in Alberta.(78) Existing consumer protection legislation in Nova Scotia,(79) Manitoba,(80) and Saskatchewan(81) has also been amended and supplemented with regulations to provide protection for consumers purchasing goods and services over the Internet.(82)

Many of the changes are based on an *Internet Sales Contract Harmonization Template*(83) developed by an Industry Canada Consumer Measures Committee in 2001, which was approved by the federal, provincial and territorial governments. This was followed by a *Canadian Code of Practice for Consumer Protection in Electronic Commerce*,(84) which was endorsed by federal, provincial and territorial ministers responsible for consumer affairs in 2004.

These new initiatives are focused on certain common principles, including the following:

- Internet vendors should provide accurate and sufficient information to consumers seeking to transact with them.
- All disclosures should be provided in any language in which goods and services are also proffered.
- A consumer's consent to an Internet contract must be fully formed and intentional, with a meaningful opportunity to cancel or correct orders.
- Internet vendors should adhere to generally accepted standards for protection of their customers' privacy and personal information.

---

(76) *Consumer Protection Act, 2002*, S.O. 2002, c. 30, Schedule A.

(77) *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2.

(78) *Internet Sales Contract Regulation*, Alta. Reg. 81/2001.

(79) *Consumer Protection Act*, R.S.N.S. 1989, c. 92.

(80) *Consumer Protection Act*, R.S.M. 1987, C. C200.

(81) *Consumer Protection Act*, S.S. 1996, c. C-30.1.

(82) Freedman and Copland (2008), p. 342.

(83) Industry Canada, Canada's Office of Consumer Affairs, *Internet Sales Contract Harmonization Template*, 25 May 2001, http://www.ic.gc.ca/eic/site/oca-bc.nsf/en/ca01642.html.

(84) Consumer Measures Committee, *Canadian Code of Practice for Consumer Protection in Electronic Commerce*, 2004, http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00064e.html.

- Internet vendors should use security mechanisms adequate to protect storage of customers' personal information.

- Consumers should be provided with access to a process for complaints and dispute resolution.

- Consent should be given by customers for any unsolicited marketing e-mails.

- Internet communications and transactions with children should be subject to strict and careful standards, including a requirement that no monetary transactions or collection of personal information be conducted without the consent of a parent or a guardian.(85)

Other areas of regulation that are currently in development relate to advertising over the Internet, cybercrime, e-securities, Internet domain names, and the application of taxes to e-commerce. Further updated information on all of the existing laws and legislative initiatives in these areas in Canada, as well as the full text of the e-commerce and Internet consumer protection laws discussed in this paper, can be found together in the annual edition of the *Consolidated Electronic Commerce Statutes and Regulations With Related Materials*, published by Thomson Carswell.(86)

CONCLUSION

The move to pass legislation to integrate the world of electronic communication into long-standing legal requirements for written communications, signatures and the formation of contracts started with the UNCITRAL Model Law on Electronic Commerce in 1996, the creation of model laws in Canada and the United States in 1999, and the directive of the European Union in 2000. Now, most national, state and provincial governments have enacted laws to reduce or remove the legal uncertainties surrounding the conduct of business over the Internet, and continue to develop an extensive legal framework for these transactions.

Recognizing that electronic commerce extends beyond provincial and national boundaries, Canadian governments are for the most part opting to model their legislation on the *Uniform Electronic Commerce Act*, the UNCITRAL Model Laws, and other national and international protocols. This approach acknowledges that consistent rules governing the use of

(85) Freedman and Copland (2008), pp. 345–46.

(86) Freedman and Copland (2008).

electronic documents and signatures are vital for the continued growth of business-to-business and business-to-consumer transactions over the Internet.