DIGITAL SIGNATURES: MEETING THE TRADITIONAL REQUIREMENTS ELECTRONICALLY

A CANADIAN PERSPECTIVE

Mark Lewis[*]

This paper addresses the Canadian legislative approaches designed to ensure that electronic signatures have the validity and trustworthiness required by businesses to compete in the global electronic marketplace. Part I discusses the traditional objectives of signatures and how those objectives can be met and exceeded over open networks through the application of digital signatures technology. Part II analyses recent Canadian federal and provincial strategies aimed at ensuring that Canadian businesses have a uniform legal foundation upon which they can provide both customers and other businesses with a secure means of doing business electronically. The inevitable conclusion is that Canada has, to date, failed to implement a legislative framework that develops a national systematic method for promoting secure electronic commerce transactions between parties over open networks.

I. INTRODUCTION

IN THE FAST PACED WORLD of global business a race has emerged between and within nations to capitalize on e-commerce. At stake is an estimated $1 trillion in yearly global sales.[1] At the heart of all commerce is an agreement, or contract, upon which businesses depend to enter into binding arrangements. This is no different in cyberspace, with perhaps one exception: the rules must be modified in order to deal with the unique impediments of forming a contract electronically. Those countries that adapt, facilitate, and encourage electronic contracting first will gain an advantage and provide the foundation for a strong presence in the electronic economy.

An important, yet challenging, element of an electronic contract is the need to meet the traditional requirements of a signature. The following evidences that, while electronic and traditional signatures are fundamentally different, both can fulfil the purposes underlying signature require-

[*] Gowling Lafleur Henderson LLP.

[1] G. R. Ferrera, et al., Cyberlaw: Texts and Cases (Cincinnati: Thomson Learning, 2000) at 90.

ments. Recently, Canada's federal and provincial governments have introduced bills and enacted statutes to overcome this hurdle. This paper will review these various legislative approaches to administering electronic and digital signatures in light of the inherently transborder nature of e-commerce. From this, a conclusion can be reached: the lack of uniformity for electronic signatures, intra-nationally and internationally, will severely hamper the promulgation of the digital economy.

II. CONTRACTUAL REQUIREMENTS FOR WRITING AND SIGNATURES

A. The Basics of a Contract

It is prudent to begin with a review of the basic elements of a contract in order to ascertain the essential characteristics of a signature. It will then be easier to determine which electronic approach could satisfy the purposes and requirements of a traditional signature.

The law has established that a contract is valid and enforceable if it must meets the requirements of mutual assent, consideration, capacity, legality, and form.[2] Mutual assent is often referred to as "a meeting of the minds" and is manifested by words or conduct that represents the parties' intention to enter into a contract. Normally, this is accomplished where one party makes an offer and the other party accepts it. Consideration requires that each party to the contract exchange something of value.

The parties must also have the capacity or legal ability to enter into a contract. The legality requirement is that the object of a contract cannot be criminal, tortious, or otherwise contrary to public policy.

Additionally, a number of contracts must be made in a particular form. That is, they must be in writing and they must be signed. Typically these include arrangements involving an interest in land, those not performed within one year, collateral contracts, those made in consideration of marriage, and specific contracts made by an executor or administrator.[3] Other contracts also have to meet the form criterion, including those

[2] Ferrera, *supra* note 1 at 93. Also see generally c. 5 at 90-126.

[3] These are usually set out in the various statutes of frauds across Canada and the US. For example, see: *Statute of Frauds,* R.S.O. 1990, c. S.19. Note that in Canada a number of jurisdictions have repealed the statute of frauds, including Manitoba.

for the sale of goods to consumers[4] and those for the lease of goods over a specified monetary amount.[5] The form requirement is designed to ensure that there is tangible evidence that the contract was made. Usually, provisions nominate specific parties, outline the subject matter or essential terms, or demand a signature to be witnessed by others. Notably, national and international sale of goods legislation and trade agreements do not have form requirements for commercial arrangements.[6]

Regardless of these statutory requirements, there is a general bias in the law towards encouraging the reduction of parties' intentions to agreements written on paper and endorsed by a signature. With electronic contracts, this reduction is fundamentally different. In order to determine the best way to overcome the dissimilarities, a review of the basic purposes of writing and signatures in contracts is necessary.

B. Purposes Underlying the Requirements for Writing and Signatures

There are three legal purposes that electronic contracts must meet: authenticity, integrity, and non-repudiation. These purposes are satisfied through writing and signatures.

1. Writing

The purpose for the writing requirement is to ensure the preservation of the terms of a contract in a semi-permanent fixed medium. For example, the Uniform Commercial Code (UCC) defines writing as "any intentional reduction to a tangible form, including printing and typing."[7] Such evidence ensures that there is protection against the various memories

[4] *Consumer Protection Act*, R.S.O. 1990, c. C31, s. 19: an executory contract must be signed by the parties; *The Consumer Protection Act*, R.S.M. 1987, c. C200, ss. 4(2), 5(2), and 5(13): sales involving costs of borrowing, hire purchases, and most loans, respectively. There is a general requirement that contracts be written and signed for retail transactions over a specified period amount.

[5] *Uniform Commercial Code*, c1999, ss. 2-201(1), 1-1206, and 2A-201. Hereafter referred to as UCITA.

[6] *The Sale of Goods Act*, R.S.M. 1987, c. S10; *Sale of Goods Act*, R.S.O. 1990, c. S1, s. 4; and the *United Nations Convention on Contracts for the International Sale of Goods (Vienna Sale Convention)*, 11 April 1980, online: UNCITRAL <http://www.uncitral.org/english/texts/sales/CISG.htm>.

[7] *Supra* note 5 at 1-201(46).

and recollections of the parties to an agreement. Therefore, if an agreement is in a medium that preserves the intention of the parties, the writing requirement would be satisfied; following this, a computer record should suffice. Ultimately, a contract is a powerful instrument that an adjudicator can use to determine the intentions of the parties, and to evidence authenticity, integrity, and non-repudiation.

2. Signature

A signature evidences a present intention by a specific party to accept or verify a document or agreement through the adoption or execution of any symbol.[8] Therefore, a signature need not be made in ink. Canadian and American courts have held that signatures include names on telegrams,[9] telexes,[10] typewritten names,[11] letterheads,[12] and faxed signatures.[13] In *Re Newbridge Networks Corp.*, Farley, J., for the Ontario Superior Court of Justice, affirmed this by stating:

> What of the electronic signature? I think that aspect is answered by analysing what is intended to be the signature.... It would seem to me that an electronic signature with the integrity of passwords would be easier to verify [than a traditional signature].... If I execute an electronic signature, that is too my signature as I *intend* it to be my signature (and the recipient is so advised of that intention in the context).[14] [Emphasis added.]

[8] *Ibid.* at 1-201(39).

[9] *Hillstrom v. Gosnay* (1980), 614 P. 2d 466.

[10] *Hideca Petroleum Corp. v. Tampimet Int'l Ltd.* (1987), 740 S.W. 2d 838.

[11] *Watson v. Tom Growney Equip. Inc.* (1986), 721 P. 2d 1302. A name typed on a purchase order was found to be a sufficient signature since the signatory had deliberately filled out other details on the form.

[12] *Kohlmeyer & Co. v. Bowen* (1972), 192 S.E. 2d 400. A securities brokerage firm's name was printed on a confirmation statement for the sale of securities. The Court found the printed name was intended as authentication, and met the signature requirement under the statute of frauds.

[13] *Beatty v. First Exploration Fund 1987 and Co.*, [1988] B.C.J. No. 666. Hinds J, held that faxed signatures on proxy documents were sufficient to meet the signature requirements under a limited partnership agreement.

[14] [2000] O.J. No. 1346 at para. 6-7.

Accordingly, a name at the end of an email, or anything else that is intended to be a signature would suffice.

A signature is not part of the substance of a transaction, but rather of its representation or form. The American Bar Association (ABA) has identified four purposes for a signature: evidence, ceremony, approval, and efficiency and logistics considerations.[15]

a. Evidence

A signature authenticates writing by identifying the signor with the signed document. When the signor makes a mark in a distinctive manner the writing becomes attributable to the signor. Therefore, the evidence requirement means that there must be some clear association between the characteristics of a signature and the signor to prove the authorization.

b. Ceremony

The act of signing a document calls to the signor's attention the legal significance of the signor's act, thereby helping to prevent "inconsiderate engagements." It demonstrates that there was some level of comprehension and understanding of the legal obligations of the document.

c. Approval

In certain contexts, defined by law or custom, a signature expresses the signor's approval or authorization of the writing, or the signor's intention that it have legal effect. In essence, a signature represents the acceptance of the terms contained within the writing.[16]

[15] Electronic Commerce and Information Technology Division Section of Science and Technology, Information Security Committee *Digital Signature Guidelines (DSG) Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (American Bar Association 1995, 1996) at 4.

[16] This has been followed in Canadian courts. See *Summer* v. *Sapkos and Janelunas* (1955), 17 W.W.R. 21 at 23 where it was held:

> In the absence of proof of fraud a person who is informed of the contents of a document the full effect of which he does not understand may be bound by it if he signs it even though illiterate.

d. Efficiency and Logistics

A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of the document. For example, negotiable instruments rely upon formal requirements (including a signature) to enable them to change hands with ease, rapidity, and minimal interruption.

For an electronic signature to satisfy the purposes of a traditional signature two requirements must be met. These include authentication and integrity.[17]

i. Authentication

A signature should indicate who signed a document and should be difficult for anyone else to produce. Because electronic signatures are not inherently unique it is difficult, if not impossible, to determine if the person with the authority actually signed a document.

ii. Integrity

A signature should identify and verify what is signed to the extent that there is a degree of inseparability between the instrument and the signature itself.

Through the application of authentication and integrity non-repudiation occurs where there is:

> assurance of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received, or to protect against false denial by the sender that the data has been sent.[18]

Also, as stated by MacDonald, J. of the British Columbia Supreme Court in *Crown Packaging Ltd. v. Royse Sports Ltd.*, [1997] B.C.J. 1421:

> In *Marvco Color Research v. Harris*, [1982] 2 S.C.R. 774, at p. 785, it was held that the defence of non est factum is not available to a person who fails to exercise reasonable care in signing a document, as against one who relies on the document in good faith and for value.

[17] T. J. Smedinghoff, "Electronic Contracts & Digital Signatures: An Overview of Law and Legislation" 564 PLI/Pat 125 at 147.

[18] *Supra* note 15 at 7.

Where the purpose of a traditional signature has been to indicate intent, acceptance, and verification by a specific person, authentication via a secure electronic signature can conceptually be equally useful. Instead of applying a signature to a document with ink, one would apply an electronic signature to a document by a process.[19]

A process is required because, as previously mentioned, there is nothing inherently unique to an electronic signature. It is nothing more than a series of "ons" and "offs" represented by "ones" and "zeros." A person is thereby unable to differentiate between an honest and a forged electronic signature. Herein lies the difficulty for parties that need to be sure that the signature belongs to a party with the authority to sign the document, thereby making it enforceable. How can electronic signatures overcome the lack of paper-based indicia of trustworthiness?

The answer to this dilemma lies in a "security procedure," defined as a methodology or procedure used for the purpose of (1) verifying that an electronic record is that of a specific person, or (2) detecting error or alteration in the communication, content, or storage of an electronic record since a specific point in time.[20] While there are a number of security procedures available, the most developed and widely used procedure at present is that of the digital signature.

III. DIGITAL SIGNATURE TECHNOLOGY

A. The Digital Signature Process

Although used interchangeably by many, there is a difference between an electronic signature and a digital signature. An electronic signature is any symbol created electronically which is intended to be a signature, whereas a digital signature is a means of verifying and authenticating a document by having a computer create a unique identifier through the application of encryption or encoding. A digital signature does more than ensure a means of identifying a specific signor, it also ensures that the signature is for a specific document and that the document has not been tampered with.[21]

There are two widespread types of cryptography in use today: symmetric and asymmetric cryptography. Symmetric cryptosystems rely upon privacy and confidence between two parties who share a single key

[19] D. L. Kidd, Jr. and W. H. Doughtrey, Jr., "Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions" 26 Rutgers Computer & Tech. L.J. 215 at 253.

[20] Smedinghoff, *supra* note 17 at 144.

[21] See *supra* note 15 at 8-13 for a complete discussion of this technology.

for both encryption and decryption. An example of this system is a bank card and the corresponding personal information number (PIN) which is known by both the bank and the client. The problem with symmetric cryptosystems is that they do not lend themselves to secure communications between many unknown, and perhaps untrustworthy, parties. For this reason asymmetric cryptosystems (also known as public key encryption) were developed.[22]

Because all information entered into a computer is read as binary digits, a computer is able to perform mathematical functions on the numbers. As a result, messages can be transformed into alternate representations unique to the original message. A digital signature involves two keys assigned to a single person, one referred to as the "public key," and the other referred to as the "private key." The public key is available to the populace, while the private key is held exclusively by a person and should not be shared or disclosed. When a person signs a document electronically, the signature is encrypted using the private key. When the transmission is received the private encryption can be decoded using the public key. Although the keys are related, each one performs the inverse function of the other. Therefore, it is mathematically improbable that they could be derived from each other. In other words, what one key does the other key can only undo.[23]

The creation of a digital signature involves the application of two algorithms: a hash algorithm and a signature algorithm. The algorithms are complex mathematical equations employed on the original message to give it an alternative representation. The "hash function" or "session key" is performed first. A "hash function" is:

> [an] algorithm which creates a digital representation or "fingerprint" in the form or a "**hash value**" or "**hash result**" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it.[24] [Emphasis in original.]

The "hash function" is applied to the original binary code resulting in a message digest that is normally a 160-bit string of digits unique to the original message. It is a randomly created formula which is included in the packet of information sent to the recipient. The effect is that for every

[22] *Ibid.*

[23] *Ibid.*

[24] *Ibid.*

message there is a specific hash value and any modification to a message would result in a different hash value.[25]

Next, the private key or signature algorithm is applied to the message digest resulting in the digital signature. Figure 1 is a simple illustration of how a digital signature is created.[26]

FIGURE 1
CREATION OF A DIGITAL SIGNATURE

Creation of a Digital Signature

ORIGINAL MESSAGE	10
HASH ALGORITHM	x2
MESSAGE DIGEST	20
SIGNATURE ALGORITHM	x4
DIGITAL SIGNATURE	**80**

The digital signature (numerical value 80) would be sent to the recipient along with the original message and with the specific hash algorithm applied in the encryption process.

Through the application of this process a digital signature transforms the original message using a "secret" known only to the signor (the private key), thereby unique to both the signor and the message being signed. Any change in data (even one character) would result in a different message digest and subsequently, a different digital signature.[27]

The decryption of the digital signature occurs when the recipient receives the message. It is decoded using the public key to produce the message digest. Concurrently, but separately, the hash algorithm included in the message packet is applied to the original message to produce the message digest. If the two message digests match then the message is authenticated, thereby proving the message has not been tampered with. Alternatively, if the digests are not the same the message is a forgery. An example of the decryption process is found in Figure 2.[28]

[25] *Ibid.*

[26] *Ibid.*

[27] *Ibid.*

[28] *Ibid.*

FIGURE 2
DECRYPTION OF A DIGITAL SIGNATURE

Decryption of a Digital Signature

DIGITAL SIGNATURE	10	ORIGINAL MESSAGE	10
PUBLIC KEY	/4	HASH FUNCTION	x2
MESSAGE DIGEST	20	MESSAGE DIGEST	20

The public key is applied to the digital signature to give the message digest. The message digest must be identical to that produced when the included original message has the hash function applied to it.

The preceding discussion shows that the digital signature is inherently part of that particular message and that the message is inherently part of the digital signature. Therefore, a digital signature allows a recipient to determine if a specific person has "signed" a specific document, and whether there has been any modification to it in transit or at any other time since it was digitally signed. In this way, through two processes, digital signature technology overcomes the impediments of authenticity and integrity while also establishing non-repudiation. A digital signature is not truly a signature at all, but rather, is a process of encoding a document that uniquely identifies an individual. For a representation of the digital signature processes see Figures 3 and 4.

FIGURE 3
DIGITAL SIGNATURE CREATION PROCESS

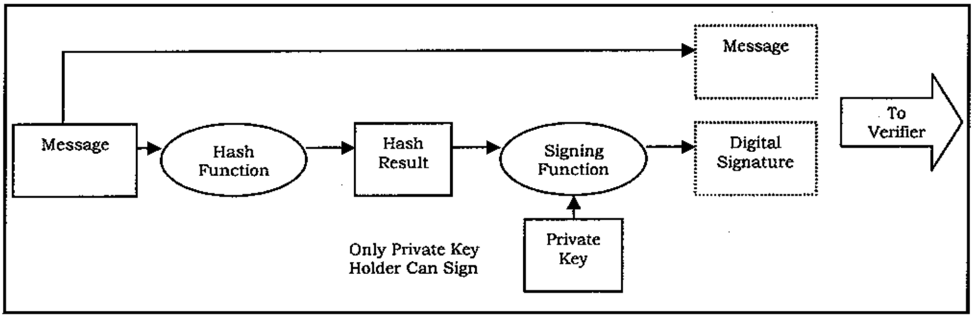
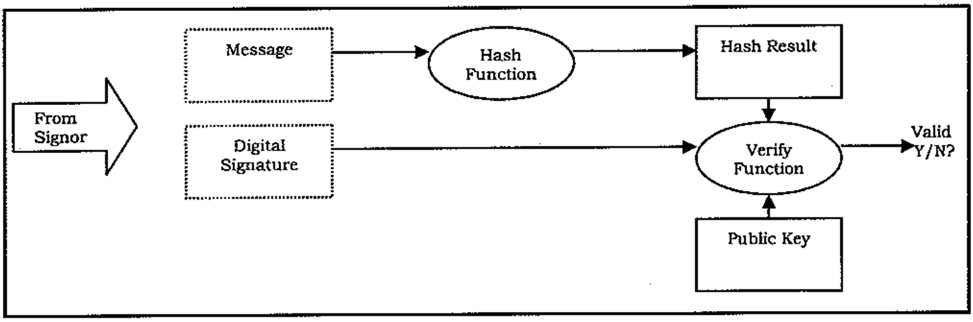


FIGURE 4
DIGITAL SIGNATURE VERIFICATION PROCESS



There is one crucial problem with the digital signature process: how can one be sure that the key pairs are those of the person "signing" a document? There must be a method to ensure that an assigned digital signature belongs to the person it is supposed to belong to. This can best be accomplished through the creation of a certifying authority (CA).[29]

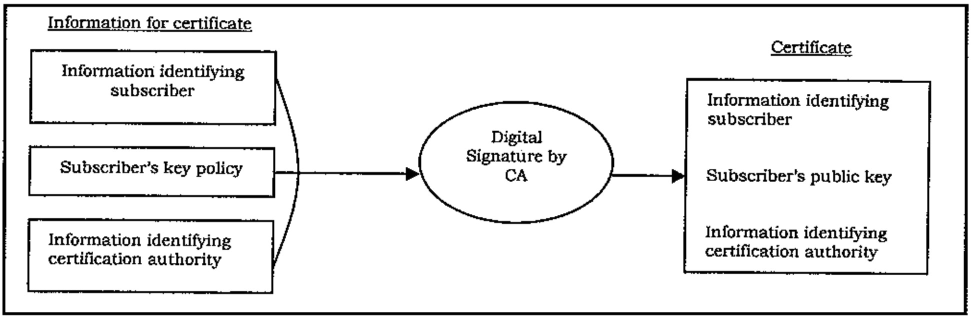
A CA is a third party who is trusted by both the sender and the receiver to ensure that the person sending and digitally signing a document is the person he or she claims to be. This is accomplished by ascertaining and verifying the identity of a person and, thereafter, certifying that the public key truly belongs to him or her. It is suggested that this involve the four steps as illustrated in Figure 5:[30]

> 1. A person, referred to as the subscriber, generates his or her own public/private key pair;
> 2. the subscriber contacts the CA and produces proof of identity; and
> 3. the subscriber demonstrates that he or she holds the private key which corresponds to the public key without disclosing it; and
> 4. the CA publishes a certificate that assures the public that the person who holds the key pair is the person that he says he is.

[29] At present there are a number of private CA's. For example: "VeriSign," online: VeriSign <http://www.verisign.com> and "Digital Signature Trust Company," online: Digital Signature Trust Company <http://www.digsigtrust.com>.

[30] *Supra* note 15 at 15.

FIGURE 5
CREATING A CERTIFICATE


Information for certificate
Information identifying subscriber
Subscriber's key policy
Information identifying certification authority
Digital Signature by CA
Certificate
Information identifying subscriber
Subscriber's public key
Information identifying certification authority

Certification involves the assigning of a certificate that "is a computer-based record that attests to the connection of a public key to an identified person or entity."[31] To ensure that the certificates are authentic a CA digitally signs each certificate that it creates. In order for CA's to prove their own identity, they must have another CA sign their certificate and so on. This hierarchical means of verifying identities is referred to as "chaining certificates."[32] Ultimately, it must reach a point where parties can reasonably be assured of the required identities. At the top of the echelon a public body, or other highly trusted entity, is required to safeguard the certificates below it in a manner that is in the best interests of all parties.[33]

The preceding discussion demonstrates that digital signatures meet the purposes of a signature better than traditional signatures do. They ensure authenticity, integrity, and non-repudiation. Additionally, the technology is readily available. To ensure that people and businesses between jurisdictions can equally rely on digital signatures there must be uniformity of both technology and infrastructure. This can best be established through legislation, although there is ample debate surrounding how much the government should be involved. The remainder of this paper will examine the Canadian approach taken on this topic at both the federal and provincial levels of government.

[31] Smedinghoff, *supra* note 17 at 150.
[32] *Ibid.* at 153.
[33] For an example of this approach see *Utah Digital Signature Act,* (1995) § 46-3, online: Utah Digital Signature Act <http://www.jmls.edu/cyber/statutes/udsa.html>.

IV. LEGISLATIVE APPROACHES TO ELECTRONIC SIGNATURES IN CANADA

A. Overview

Over the past six years governments around the world have been racing to enact legislation to address the exploding area of e-commerce. Many of these statutory instruments have been designed to address the particular area of electronic signatures. Due to haste, and a lack of international and national consensus, approaches to legislating in this area are diverse. Generally, they can be divided into three categories:

1. Technology Neutral:

> [t]hese statutes give legal effect to any electronic signature, but they allow a court to decide what evidentiary weight to give the signature based upon the security of the technology utilized.

2. Semi-Specific:

> [t]he second category of statutes specifies that a valid signature must have certain security attributes, but does not require a particular technology. Such statistics tend to require the attributes of PKI [public key infrastructure) - digital signatures, such as user authentication and message-alteration prevention.

3. Digital Signature:

> The third group of statutes specifically requires the use of PKI-digital signatures. [Often, the government is directly involved in choosing or creating bodies to fulfill the role of Certifying Authorities.][34]

Canadian legislation falls into the first two categories. As will become evident, this places an undue strain on both the judiciary and private sector to regulate and homogenize the nebulous area of electronic signatures.

[34] W. E. Lupton, "The Digital Signature: Your Identity by the Numbers" 6 Rutgers J.L. & Tech. 10 at 35.

In Canada, laws concerning electronic signatures have been included in legislation dealing with all aspects of electronic commerce including communication, validity, and privacy. The following discussion will look at the approaches to electronic signatures in the statutes of the federal government,[35] and the provincial governments of Manitoba[36] and Saskatchewan.[37] For further illustration, proposed legislation from Ontario[38] and British Columbia[39] will also be considered. Throughout, there will be reference to the model laws and directives upon which the instruments were created, including the Uniform Electronic Commerce Act (UECA) by the Uniform Law Conference of Canada (ULCC),[40] "Digital Signatures, Certification Authorities and Related Legal Issues"[41] by the United Nations, and the "Digital Signatures Guidelines"[42] of the ABA.

B. The Definition of an Electronic Signature

Definitions of an electronic signature are homogeneous in Canadian legislation because they have been taken directly from the UECA:

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

[36] *The Electronic Commerce and Information, Consumer Protection Amendment and Manitoba Evidence Amendment Act* (ECA), S.M. 2000, c. 31.

[37] Bill 38, *The Electronic Information and Documents Act,* S.S. 2000. Note that as of the date of this publication, the Act had been assented to but not proclaimed.

[38] Bill 88, *An Act to promote the use of information technology in commercial and other transactions by resolving legal uncertainties and removing statutory barriers that affect electronic communication,* 1st sess., 37th Parl., Ontario, 2000. (Hereinafter referred to as "Bill 88.")

[39] Bill 32, *The Electronics Transactions Act,* 4th sess., 36th Parl., British Columbia, 2000.

[40] *Uniform Electronic Commerce Act* (UECA) - Annotated, was created in 1998 by the Uniform Law Conference of Canada to implement the principles of the *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment,* (1996) 51/162, online: UNCITRAL <http://www.uncitral.org/English/texts/electcom/ml-ecomm.htm>. UECA is referred to as minimalist legislation because it is a framework upon which each jurisdiction can build to create legislation that meets each province and territory's needs, policies, and goals.

[41] "Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues by the United Nations Commission on International Trade Law," UNCITRAL Note by the Secretariat, Working Group on Electronic Commerce, Thirty-first session, NY: February 1997 at 18-28.

[42] *Supra* note 15.

> "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.[43]

The meaning subscribes to the same purposes that a traditional signature does; that is, to evidence intention with respect to a particular document. However, there are some subtle, yet important, differences. First, the electronic signature is information in "electronic form" which precludes the need for it to look like, or be created like, a traditional signature. Second, the normal method by which a signature is attached to a document does not preclude the means by which an electronic signature is attached to a document. The Personal Information Protection and Electronic Documents Act (PIPEDA) further delineates the meaning of "electronic" by stating that it is "one or more letters, characters, numbers or other symbols in digital form."[44]

These provisions systematically cover any means of "signing" a document electronically, thereby providing that anything a person does electronically which is intended to be a signature will suffice.

C. The Legal Effect of an Electronic Signature

All of the Canadian legislation endeavours to legally empower an electronic signature with the same standing in law as a traditional signature. Because of the division of powers in Canada PIPEDA only applies to the federal legislation listed in Schedules 2 and 3 of the Act.[45] Concurrently, the provincial legislation only applies within that province's jurisdiction. To provide electronic signatures with legal standing all of the legislation stipulates something similar to the following:

> Signatures
> 11(1) If there is a requirement under law for the signature of a person, that requirement is satisfied by an electronic signature.[46]

[43] *Supra* note 40, s. 1(b). See also *supra* note 36 at s. 1(1); *supra* note 35 at s. 31(1); and *supra* note 37 at cl. 3(b).

[44] *Supra* note 35 at s. 31(1).

[45] *Ibid.* at s. 43.

[46] *Supra* note 39 at cl. 11(1).

Unequivocally, this provision makes an electronic signature function as a signature in law. This leads to the logical question of whether an electronic signature is to be seen as the same as a traditional signature where a signature is not required by law. By inference this would appear to be true, however, none of the legislation states this. For instance, most commercial transactions by law do not require a signature.[47] Does this mean that an electronic signature will suffice or not? This uncertainty is problematic and is likely to result in litigation or legislative amendment in order to clarify the law.

A further question arises: what happens when there is an intention to sign but the electronic signature does not meet the requirements of the legislation? Does a judge thereby have the power to say there is no binding contract? This is another matter that will require clarification in the near future.

D. The Technology Neutral and Semi-Specific Approaches

No Canadian legislation, existing or under development, fits into the third category of legislation requiring the specific use of digital signature technology. Only one statutory instrument, PIPEDA, fits into the second category by requiring that the technology used contain certain security attributes.

PIPEDA is the only legislation that has included a definition for a secure electronic signature, synonymous to that of digital signatures:

> "secure electronic signature" means an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1).[48]

Under PIPEDA the specific security precautions that must be met are set out in s. 48(2):

> Characteristics
> (2) The Governor in Council may prescribe a technology or process only if the Governor in Council is satisfied that it can be proved that
> (a) the electronic signature resulting from the use by a person of the technology or process is *unique* to the person;

[47] *Supra* note 6.

[48] *Supra* note 35 at s. 31(1).

> (b) 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;
> (c) the technology or process can be used to *identify* the person using the technology or process; and
> (d) 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.[49] [Emphasis added]

From the previous discussion of digital signatures it is evident that the characteristics in section 48(2) are the same characteristics of public key encryption. Further, the governor in council may, at his or her discretion, choose a process such as PKI-digital signatures and designate certificate authorities and other bodies to operate the technology:

> 50(2) Without restricting the generality of subsection (1), the regulations that may be made may include rules respecting any of the following:
> (e) the technology or process to be used to make or verify an electronic signature and the manner in which it is to be used.[50]

This is in contrast to the provincial statutory requirements that do not go to the same lengths in stipulating a particular process or a detailed list of characteristics that an electronic signature should possess. Alternatively, provincial statutes refer to the "reliability in view of the relevant circumstances" of the signature being identifiable with both the specific person and the particular document in question.[51]

The provincial instruments entitle the Lieutenant Governor in Council to create regulations that effectuate this goal, but there are no further directions such as the type of process that should be employed. Until regulations are created, this determination is left to the decision-maker involved, such as an arbitrator or a judge. Additionally, the provincial leg-

[49] *Ibid.* at s. 48(2).

[50] *Ibid.* at s. 50(2)(e).

[51] For example see *supra* note 39 at cls. 21(2)(d) and (e); *supra* note 36 at s. 13(1)(a); and *supra* note 32 at cl. 14(2)(b).

islation empowers the Lieutenant Governor to create regulations or schedules that prescribe records or classes of records to which the legislation applies.[52]

Manitoba's legislation goes further than any other province by giving the lieutenant governor the power to create regulations that specify the particular method or process that would be acceptable for electronic signatures:

> 18(1) The Lieutenant Governor in Council may make regulations
> (d) respecting electronic signatures, including
> (ii) prescribing methods or processes, or criteria for determining acceptable *methods* or *processes*, for applying electronic signatures, which may be different for different types of documents.[53] [Emphasis added.]

Overall, the Canadian method can be characterized as a broad-based approach that requires no specific technology to meet the requirements of a reliable electronic signature. There is no mention of CA's, certificates, or digital signatures per se. The only statute that comes close to legislating digital signature technology is PIPEDA, but it too falls short. It fails to discuss how secure electronic signature technology is to be applied or whether PKI-digital signature technology is the process to be used.

The semi-specific and technology-neutral approaches fail to provide a consistent infrastructure by which digital signatures from other jurisdictions can readily and easily be relied upon. These methods place a large burden on parties themselves to do sufficient research to ensure that an electronic signature is reliable. The alternative is to wait until a problem arises and be forced to adjudicate then.

The legislative requirements are not sufficiently clear. Therefore, they will create substantial hurdles to facilitating ease of business arrangements between parties in different jurisdictions. Undoubtedly, the problems will result in increased litigation. Setting out a specific technology, such as PKI-digital signatures, how CA's will come to exist, and how they will be regulated, could have precluded many of the problems that now exist. What is required is not simply a listing of characteristics an electronic signature should possess, but what technology should be implemented in creating the signature itself. Although the present approach

[52] For example see *supra* note 39 at cl. 21(2)(d); *supra* note 36 at s. 18(1)(d)(i); *supra* note 37 at cls. 24(c) and (d); and *supra* note 35 at Schedules 2 and 3.
[53] *Supra* note 36 at s. 18(1)(d)(ii).

may have application within provincial jurisdictions, it is highly unlikely that it will be effective inter-provincially or internationally.

It is true that each Lieutenant Governor can create regulations regarding processes and technology. However, a patchwork approach will not meet the needs of businesses contracting from foreign jurisdictions. The present legislation does provide governments with the flexibility to deal with rapidly changing technology without having to amend or repeal statutes. However, at the very least, a clear delineation of what the regulations should entail ought to have been included in the provisions, as they were in PIPEDA.

E. The Basis of Canadian Legislation: Uniform Electronic Commerce Act

Electronic legislation in Canada is based upon the UECA.[54] The goals of the legislation are not the problem; rather, it is the means being used to achieve them. The ULCC does not stipulate any particular technology for the production of a valid signature because it wanted to ensure that the provisions provided for flexibility: "[t]hey transform questions of capacity ('Am I allowed to do this electronically?') into questions of proof (Have I met the standard?')."[55] The UECA does mention that a test for reliability can be included in the legislation. It is understandable that the ULCC took this approach. It ensures that provinces will use the "bare bone" provisions of the UECA, thereby giving the provinces some level of uniformity in their legislation. The same approach is used in the Model Law on Electronic Commerce (UNMLEC) created by the United Nations Commission on International Trade Law (UNCITRAL). For example:

> Article 7. Signature
> (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.[56]

[54] *Supra* note 40.

[55] *Ibid.*

[56] *Supra* note 40.

The model law further stipulates that in determining whether the method used is appropriate in all of the circumstances, attention should be paid to the legal, technical, and commercial factors in play listed in Appendix.[57]

It is suggested that reliance for creating legislation dealing with electronic signatures should have been placed upon UNCITRAL's proposals for a new model law and the ABA's digital signature guidelines. As UNCITRAL only recently created a new Draft Model Law on Electronic Signatures (UNMLES)[58] it is understandable that the present rash of legislation does not follow its example. Yet soon after finalizing the UNMLEC in December of 1996, a proposal was created for its modification:

> It was stated that the establishment of digital signature laws, together with laws recognizing the actions of "certifying authorities" (hereinafter referred to as "certification authorities"), or other persons authorized to issue electronic certificates or other forms of assurances as to the origin and attribution of messages "signed" digitally, was regarded in many countries as essential for the development of electronic commerce. The ability to rely on digital signatures would be a key to the growth of contracting as well as the transferability of rights to goods or other interests through electronic media.[59]

Additionally, the ABA guidelines:

> ...set forth the basics of digital signature technology, and examines how, with some legal and institutional infrastructure, digital signature technology can be applied as a robust computer-based alternative to traditional signatures.[60]

The guidelines suggest that presently the best measure for meeting the requirements of traditional signatures in an electronic format is the digital signature. Yet the ULCC failed to apply either of these suggestions in

[57] *Ibid.* at para. 58.

[58] *Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures*, UNCITRAL Note by the Secretariat, Working Group on Electronic Commerce, Thirty-eighth session, NY: 12 - 23 March 2001, A/CN.9/WG.IV/WP.88, online: UNCITRAL <http://www.uncitral.org/English/workinggroups/wg_ec/wp-88e.pdf>.

[59] *Ibid.* at para. 2.

[60] *Supra* note 15 at 3.

creating its model legislation. The result is that Canadian provinces have been left in disarray and out of touch with the present and future climate of electronic signatures. This is evidenced by the UNMLES, which lists the characteristics that an electronic signature should have and sets out the requirements and duties of CA's.[61] Although not specific in advising the use of PKI-digital signatures, the UNMLES specifies qualities that meet the traditional requirements of signatures electronically.

V. CONCLUSION

THE LARGEST OBSTACLE FACING CONTRACT FORMATION in e-commerce is the need for security, especially on open systems such as the internet. PKI-digital signature technology is capable of alleviating those fears by ensuring that persons know whom they are dealing with, while at the same time ensuring that documents have not been tampered with. Its application goes beyond signatures in contracts. Ultimately, PKI-digital signature technology is a means by which parties can gain comfort and security in transactions, agreements, and communication.

In order for the proliferation of online contracting to occur, there needs to be an infrastructure in place that is similar throughout varying jurisdictions. This will allow persons to easily verify each other's identity and facilitate e-business. The present wave of international legislation is clearly moving in the direction of requiring PKI-like technology as a basis upon which national and international commerce can take place electronically.

In Canada there is a patchwork approach to creating this infrastructure. Provincial legislation at present does not delineate with certainty what requirements a signature needs to suffice as an electronic signature. Suggesting that the requirements can be met by any symbol digitally made and placed in, or associated with, a document is insufficient. There needs to be a more definitive description of acceptable processes and, perhaps more importantly, the characteristics that they must have. At present, as the rest of the world races ahead, Canadian provinces are being left behind. By creating an environment in which consumer and commercial confidence can exist, the free flow of goods and services will be encouraged in cyberspace.

[61] *Supra* note 58, Article 6 – Compliance with a requirement for a signature.

APPENDIX A

FIGURE 6
THE LEGAL, TECHNICAL, AND COMMERCIAL FACTORS AFFECTING ELECTRONIC SIGNATURE SECURITY

1. Sophistication of the equipment used by each of the parties;
2. Nature of their trade activity;
3. Frequency at which commercial transactions take place between the parties;
4. Kind and size of the transaction;
5. Function of signature requirements in a given statutory and regulatory environment;
6. Capability of communication systems;
7. Compliance with authentication procedures set forth by intermediaries;
8. Range of authentication procedures made available by any intermediary;
9. Compliance with trade customs and practice;
10. Existence of insurance mechanisms against unauthorized messages;
11. Importance and the value of the information contained in the data message;
12. Availability of alternative methods of identification and the cost of implementation;
13. Degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and
14. Any other relevant factor.[62]

[62] *Supra* note 58.