Policy Considerations Behind Legislation Recognizing Electronic Signatures 1998

1998 Electronic Commerce

Policy Considerations Behind Legislation Recognizing Electronic Signatures

D. Bruce Farrend, Vancouver, B.C.

Introduction

The ULC is considering model legislation that would recognize electronic signatures for commercial purposes. This paper will set out my views on the policy issues that should be considered in drafting such legislation. I will leave the topic of dealings with or by government per se to others.

As a starting point, I understand there are two constraints which are more or less accepted in connection with model legislation dealing with electronic "writings" in general, to wit:

Any such legislation should, to the extent possible, be technology neutral. Any general legislation which is tied to a specific technology or process will be of limited value and may hinder electronic commerce as new technologies or processes develop.

Any such legislation should, to the extent possible, recognize electronic writings as functionally equivalent to paper based writings. In other words, rather than providing that a computer-generated document (commonly referred to as a "message") is for all purposes the same as a document written on paper, permitting legislation would provide that electronic messages can perform the same function as tangible documents.

Further, I understand that the starting point for such legislation is article 7 of the UNCITRAL Model Law on Electronic Commerce (the "Model Law"), with which I am assuming all readers are familiar.

Hence, the basic question to be addressed herein is whether article 7 is appropriate for commercial purposes and, if not, how should it be amended.

Functions of Signatures

With constraint number 2 in mind, it becomes necessary to identify the possible functions of a handwritten signature on a piece of paper (hereafter referred to as a "Pen Signature").

The only function of a Pen Signature that can be stated in general terms is to link or "bind" a person to a document. In this regard, I make no distinction between individuals and other types of persons. That is, the only blanket statement that can be made about a Pen Signature is that the signature is objective or tangible evidence that a person, in some manner, is associating him, her or itself with the document. In the context of electronic signatures, this is usually referred to as "authentication".

The Model Law (and the commentary accompanying it) suggests the functions of a Pen Signature are (1) to identify a person, (2) to provide certainty as to the personal involvement of that person in the act of signing, and (3) to associate that person with the content of the document.

With the greatest of respect to UNCITRAL, I do not accept the first function they attach to signatures, namely to identify the signer. Perhaps, if a person's Pen Signature is known to the recipient of the signed document, the signature can be used to identify the signer. I do not otherwise see how a handwritten mark on a piece of paper identifies someone. In my view, the document itself identifies the signer (or, more precisely, identifies who is intended to be the signer). A mark on a piece of paper is not evidence that a particular person signed, it is only evidence that somebody signed. Proving that a particular person signed a document or, conversely, proving that a particular person did not sign a document is not a function of the mark itself (except to the extent that handwriting analysis is used).

As to the third function identified by the Commission, I suggest that the association between a person and a document exists independently of the signature. In other words, a person first decides to associate him or herself with a document then, to evidence that fact, signs it.

The second function identified by the Commission, to provide certainty (ie. evidence) of a person's association with a document, is, in my view, the only general statement that should be made about Pen Signatures.

The nature of the association with a document, or in other words the reason for signing the document (and thereby establishing evidence of the association between the person and the document), will vary according to the nature of the document. Some examples:

- the primary function of the signature of a party to a contract on the contract is to provide evidence that the signer has agreed to be bound by the contents of the document, ie. the terms of the contract

At law, my understanding is that the signature is not deemed, or even presumed, to be evidence that the signer fully knew or understood the contents of the document, provided that the contents had not been misrepresented to the signer.

"...I have not been unmindful of the need of the Courts to restrict the plea of mistake within narrow limits because of the dangerous confusion that would ensue if a man were able to disown his own signature merely be proving that he misunderstood the contents or effect of a document. But there is ample authority, founded in good sense, that the Courts will relieve a person of his contract where a misunderstanding as to its true effect was induced, even though innocently, by the other party and where injustice would be done if performance were to be enforced."

Royal Bank of Canada v. Hale (1961) 30 DLR (2d) 138 at 150 (B.C.S.C.)

"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. If, however, the document is of an entirely different nature so that his mind does not accompany his signature, the please of non est factum applies."

Sumner v. Sapkos (1955) 17 W.W.R. 21 at 24 (Sask. C.A.)

What these two excerpts suggest is that a signature of a party on a commercial document (in the absence of fraud, forgery, misrepresentation or other such defence) effectively estops the signer from denying or repudiating the legal consequences that flow from that document. The excerpt from Sumner also supports, I suggest, my assertion that the association with a document exists independently from the act of signing it.

- the primary function of the signature of a drawer of a cheque on the cheque or the signature of a credit card holder on a credit card slip is to provide evidence that the signer has authorized the bank or credit card issuer to advance payment to somebody for the signer's account.
- the primary function of the signature on a receipt is to provide evidence that whatever is described in the receipt was, in fact, received.
- the primary function of the signature of a witness to the signature of a party to a commercial document is to provide evidence that the party, in fact, signed the document.

Some U.S. comments on the definition of "signature":

"The term "signature" includes any memorandum, mark or sign, written or placed on any instrument or writing, such as a will, with intent to execute or authenticate such instrument or writing."

In re Romaniw's Will 296 NYS 925

"The signature to a memorandum under the Statute of Frauds may be written or printed and need not be subscribed at the foot of the memorandum but must be made or adopted with declared or apparent intent of authenticating the memorandum as that of the signer."

Joseph Denunzio Fruit Co. v. Crane 79 F.Supp. 117

"A signature is whatever mark, symbol or device one may choose to employ as representative of himself."

Griffith v. Bonawitz 103 N.W. 327

Clearly, a document may serve more than one function, in which case a signature on that document would also serve more than one function. A lengthy commercial agreement may contain certifications as to matters of fact (representations), promises to do certain things (covenants), acknowledgements (receipts), authorizations (grant of power of attorney) and other matters. However, the point I am getting at is that the function of the signature is, as a general statement, determined by the document itself. I cannot imagine how a random act of signature may give rise to legal consequences in a commercial setting.

Indicate That Person's Approval

I want to emphasize this point about the association between a person and an electronic document: The nature of the association between a person and a signed document from which consequences can flow has to be ascertainable from the document itself. Recall that the Model Law provides that an electronic signature should "indicate [the signer's] approval of the information contained in the data message." The association with a document evidenced by a signature may be approval of the information contained therein or it may be much more limited. Consider three examples:

1. a document, not a word of which I approve, agree with or even believe. At the end, I might sign where it says I acknowledge having received and read the document. A silly example for sure, but the point is that my signature has a limited purpose, not having to do with approval of the information, but which is apparent from the document.
2. a proxy for a general meeting of a public company. The proxy will give the shareholder choices as to how the proxy should be voted on the various matters before the meeting. A Pen Signature on a proxy where no choices are made would be meaningless, and no consequences would flow from the delivery of that proxy. In other words, the nature of the association between the person and the document (I agree, Yes, No, Abstain or whatever) would not be ascertainable from the document. (To avoid this problem, every proxy has a default rule which typically provides that, where no choices are made, the shareholder is deemed to vote Yes to the identified matters and give discretion to the proxyholder for other matters.)
3. a witness. If I sign a document in the place marked "Witness", my association with the document is simply to provide some assurance that the named person actually signed in the place marked "Party". I am in no way approving or agreeing to the rest of the document, but my association with it is clear on the face of the document.

To beat this dead horse a little longer, in the case of a digital signature, I do not understand how the signature itself, as distinct from the data message, can indicate the signer's approval. You will recall that a digital signature is the hash result of the data message which is encrypted using the signer's private key. In other words, the signature is a product of the message, not an extra message saying "I concur with the attached message."

Where the Law Requires a Signature...

In my view, the qualifying phrase "Where the law requires a signature" decreases, rather than increases, certainty.

There are some obvious examples of the law requiring a signature in commercial and non-commercial situations. Tax returns, wills, bills of exchange and land transfers all must be signed in order to be effective. But even the obvious examples in my previous sentence are not absolute. Electronic filing of income tax returns does not involve delivering a signature to Revenue Canada. In any event, the law (which clearly includes both statutes and common law) does not typically require a signature for commercial matters. A verbal agreement is still an agreement, although proving the existence and terms of that agreement may be difficult. An agreement which has been reduced to writing but not signed is evidence of the existence and terms of the agreement. The law may apply a presumption

once the document has been signed (ie. the parol evidence rule), but an unsigned contract does not, in any general way, give rise to any presumptions.

A much murkier problem arises in private law. If the parties to a transaction agree that the terms of their transaction will be reduced to writing and signed, surely they are free to agree on the form of signature and the extent to which the identity of the person signing, the capacity of the parties and any other matter of concern might be proved. If the parties agree that their respective signatures would be guaranteed (as is the case with trust companies dealing with stock powers of attorney transferring publicly traded shares), then that agreement should prevail. The Model Law specifically provides that that would not be the case, providing instead that the reliability of the signature is determined "in the light of all the circumstances, including any relevant agreement." In other words, the Model Law allows a judge to say to a party: "I am not bound to honour your agreement, the other party's signature was good enough."

Thus, article 7 first requires that a person determine whether a signature is required by law, a knotty enough problem in itself, and then provides that a specific agreement concerning the signature will not necessarily be enforced.

At this point, I would suggest considering signatures (and hence legislation recognizing electronic signatures) in two categories:

1. where a signature is required by legislation either for "official" purposes, ie. dealings with or by government per se, such as information filings, or other purposes, such as bills of exchange; and
2. where a signature is not required by statute.

I shall, as promised, not deal with category 1 except to make the following brief observation. The level of certainty needed as to the identity of the signer will vary considerably among the various statutes and thus the "method used to identify that person" can probably be prescribed as may be necessary. In other words, I do not see how global or default rules concerning electronic signatures, the purpose of which are to remove barriers to business over the wire, can be applied holus bolus to situations where a signature is required for governmental policy or administrative reasons. Therefore, for situations where the law truly requires a signature, global legislation could simply state that, where permitted by regulation, electronic signatures could be used in place of Pen Signatures and the regulations would prescribe the method of electronically signing a message for the particular statute or government agency.

That Requirement is Met.

If, as I suggest, article 7 is twinned into a "signature required by statute" (Category A) section and a "signature not required by statute" (Category B) section, then, in the latter case, it is obviously inappropriate to speak of meeting the requirement for a signature with an electronic signature.

The issue is whether to provide for mandatory recognition of electronic signatures: "An electronic signature is as effective as a written signature if." or to remove the "prejudice"

against electronic signatures: "Legal effect shall not be denied a signature in electronic form solely on the basis that it is not in writing." Or both, depending on the circumstances. Readers will be familiar with that debate and I will not repeat it here. Suffice it to say, Category A signatures could be presumed to be "good" if the prescribed process is followed but, in the absence of a prescribed process, ie. Category B, I suggest that the most that should be attempted is to remove the prejudice against electronic signatures.

Let me explain why I used the term "prejudice" in the preceding paragraph. If I am correct in my assertion that a signature is, in a commercial context and absent any statutory requirements, only evidence of an association between a person and a document, then there may not be a legal barrier to electronic signatures. There may, in fact, simply be a perceived legal barrier. I refer to Beatty v. First Exploration Fund (1987) 25 BCLR (2d) 377, in which the B.C. Supreme Court pointed out that the federal Interpretation Act already contemplated electronic (in that case, faxed) signatures. In any event, whether the barrier to electronic signatures is legal or perceived, perception is reality and legislation should be enacted to remove all doubt.

Some might ask, in addition to Category A and Category B electronic signatures, could we not also have a Category C, namely: in the absence of a statutory signature requirement, if you follow this process (eg. secure electronic signatures), the signature will be presumed to be good? Such a provision would shift the burden of proof (ie. the risk) from the recipient of a signature onto the putative signer. To what end? The normal rule of civil procedure is that the burden of proof lies with the person alleging a disputed fact. To disturb that longstanding, and in my view sensible, rule in what I understand is intended to be enabling legislation is inappropriate in other than Category A cases.

To take even the most supportable case, of digital signatures employing strong encryption backed by licenced certification authorities, to provide such a presumption would be to say: "Once you get a certificate and post your public key, you must bear the risk of its misuse." Where that proposition is agreed to in a contract, I have no problem. For example, I have agreed with my bank that, until I tell them differently, they are entitled to assume that my electronic signature (my PIN) is binding on me. However, to provide such a presumption in global legislation would be to create a new animal, rather than simply enabling an electronic signature to be functionally equivalent to a Pen Signature.

Execution and Delivery

I have been unable to reach any steadfast conclusions regarding the issue of delivery of electronic documents and I raise it here primarily to invite consideration of the issue by readers.

Lawyers often speak of "execution and delivery" in the sense that execution refers to the act of signing a document and delivery refers to the giving of that document to someone else in order that consequences will flow from the document. Put another way, the delivery of a signed document completes, or makes effective, the signing thereof. To illustrate my point, consider an escrow arrangement. Transactions may be structured so that documents do not have effect (or, more precisely, the consequences described therein do not arise) until the

documents are released from escrow, at which time "delivery" occurs. Typically, an escrow release happens after the fulfillment of one or more conditions. Thus, a commercial document may be signed, and the purpose or purposes of the signature are apparent from the document, but which is not considered to be delivered (ie. effective or legally binding) unless and until one or more conditions are fulfilled. Those conditions may not be (and in the case of escrowed documents, typically are not) contained within the document itself.

Conversely, electronic messages are either sent or they are not. That is, the separation of execution (ie. signature) and delivery (ie. accepting the consequences of the document) may not be practical in the case of electronic messages. Is this a concern? Perhaps the answer is: if the parties to a transaction are prepared to take the trouble to structure their transaction with an escrow component (eg. storing a signed message on a third party server) or other conditional delivery, they will have addressed the delivery concerns and will not be looking to default rules to govern delivery.

The Identity of the Signer

I earlier suggested that the Model Law added a function to electronic signatures that did not exist in the case of Pen Signatures, namely to identify the party signing. In the case of electronic signatures generally, and digital signatures in particular, I suggest that this view of the world is both inappropriate and, to a degree, unnecessary.

As to inappropriate: I earlier argued that a Pen Signature is not evidence that the named person signed a document. Consider a will. In most provinces, execution of a will, unless completely in the testator's handwriting, is proved by two witnesses, neither of whom are beneficiaries. That is, the law considers the link between the testator and his will to be of sufficient importance that two people must be present at the signing so that, if necessary, they can give evidence as to that fact. The identity of the signer is proved by witnesses, not by the Pen Signature. Why is it that electronic signatures should provide proof of identity, given the quest for functional equivalence? As readers will no doubt realize, my point is that proof of the identity of electronic signers usually comes from third parties such as certification authorities.

As to unnecessary: In many cases, the identity of one or more parties to a transaction is irrelevant. Consider a very common example: If I were to purchase something at a retail store and pay for it with my debit card, the merchant would not be concerned as to my identity (except, perhaps, to put me on their mailing list). I signed something by entering my PIN into the machine, and thereby giving my bank some information but, as I will shortly explain, I did not necessarily identify myself through my electronic signature.

If I had given my debit card and PIN to my neighbour, and he used it to buy something at a store with my consent, neither the merchant nor the bank would realize that it was not me signing electronically. Thus, what the electronic signature actually does is link the document/message (in this case, the request for payment from my bank) with an attribute of mine, namely my PIN. The identity of the merchant is similarly irrelevant to the bank; it is concerned only that payment be sent to the credit of a specified bank account. In other words, only an attribute of the merchant, its bank account, is of concern to my bank.

A client of mine explained to me the following situation in which, not only are digital signatures not used to identify the parties to a transaction, they are used to conceal the identities. A firm offering adult pictures for sale on the internet would be concerned (usually in order to avoid criminal sanctions) that its customers be of a minimum age and possibly also not reside in certain jurisdictions. The actual identity of its customers would not be of concern to it, provided the age and residence requirements were met. A person wishing to purchase those adult pictures may not wish his identity known to the purveyor or to eavesdroppers (assuming that the purchase order is not encrypted). Thus, the purchaser may obtain from his CA a certificate linking his public and private keys and tying them, not to his name, but to two of his attributes, namely his age and jurisdiction of residence.

Thus, I suggest that, where the identity of a party to a document is relevant, the document itself will identify the party. Evidence that the party actually signed it comes from a source other than the signature. Where the identity of a party is not relevant for the purposes of the transaction, there should be no need for the signature to have to include the signer's identity.

Proof of Attributes

In the ordinary course of business in the real world, we often do not consciously require any evidence as to the attributes (typically, the identity) of someone signing a piece of paper. Whatever evidence we get often comes from the context of the message. On the other hand, if evidence of attributes is important, we, the recipients of a signature, take such steps as are necessary to obtain a level of comfort. Consider the following three examples of transactions to which I was a party recently:

1. I subscribed for a (thoroughly wholesome and educational) magazine by filling in an electronic form at a Website, including my credit card number, and emailing it to the publisher.
2. I enrolled in a course at a local college by telephoning the school and giving my name and credit card number. Quare: is a verbal authorization a form of electronic signature?

In neither case did the vendor ask me for a single piece of information which would verify my identity. Further, both organizations accepted the risk that I was not who I said I was and that I was not authorized to use that particular credit card.

In the case of the magazine, I expect that the publisher believed that the holder of a stolen credit card would not use it to place a $36 subscription for a magazine and give a mailing address. That was good enough for him. Even if the card were stolen, and the charges reversed by my bank, his downside is the cost of one copy of the magazine mailed to my home. In the case of the college course, I expect that a similar rationale (conscious or otherwise) lay behind the lack of any inquiry into my identity or other attributes (ie. "authority to use that particular credit card-ness").

1. In order to renew my "residents only" street parking permit from the City of Vancouver, I was required to present myself together with two pieces of identification showing that I, in fact, resided in the neighbourhood. The City required a high level of comfort concerning my "live in the area-ness." A completely unlikely

> and cynical reason for its concern might be to maintain employment opportunities for unionized municipal employees but really the City was concerned about the social evils inherent in a raging black market for street parking permits.

The point is this: Persons accepting a signature now seek such evidence as to the identity or other attributes of the signer as they consider appropriate, based on the amount of harm that would be expected if the particular attribute did not belong to the signer. Except in certain limited, and prescribed, cases, there is no legal presumption that a signature is "genuine" or "valid". An exception that springs to mind is the presumption contained in the Evidence Act as to the genuineness of a judge's signature on an order.

Hence, the issue to be addressed is: should electronic commerce legislation provide a presumption that an electronic signature (or a sub-class thereof, the so-called secure electronic signatures) is what it purports to be? I have earlier argued against creating a general presumption to that effect. In Category A cases, it might be appropriate, even if simply for administrative purposes, to impose an obligation on users of a prescribed electronic signature process to monitor the use of their signature and thereby create a basis for such a presumption. However, in Category B cases, I suggest that creating such a presumption, even if limited to secure electronic signatures however defined, would be to create a new "thing" which is not functionally equivalent to a Pen Signature but is, in fact, of enhanced functionality. If, however, a person wishing the ability to use an electronic signature, secure or otherwise, agrees that he, she or it will bear the risk of its misuse, courts should, as they do now in other cases such as my debit card, honour that agreement.

What, then, of licencing certification authorities, assurance bonds and all that? I suggest that that is a separate topic, certainly not unrelated but at the same time not integral to enabling electronic signatures.

Certification authorities might want to be licenced to enhance their perceived legitimacy, but it is not necessarily necessary. It is my understanding that the world's largest CA, Verisign, achieved that status in the absence of any statutory licencing scheme. While not a traditional certification authority, the chartered accountants and certified public accountants have developed a programme called WebTrust to audit the business practices of web-based merchants, again in the absence of any statutory licencing scheme.

Public key infrastructure is based upon a hierarchy of CAs. That is, you verify the attributes of a certificate by moving up the chain of CAs until you find one you trust. A licencing scheme simply has government as the root CA. How far up the hierarchy of CAs I want to check before accepting a digitally signed document is up to me, based upon the level of comfort I want which, in turn, is based upon the downside of accepting an invalid signature. If I went all the way to the government CA, how do I know it really is the government? Perhaps the hash result of its public key is published in the Gazette. How do I know the Gazette printed the hash result correctly? At some point, I have to trust somebody or, if I don't, then it is entirely up to me not to accept an electronic signature.

Approval of the Information Contained

I have made the point many times herein that a signature provides evidence of an association between a person and a document, the nature of which association is contained in the document. If I sign a contract, cheque, income tax return or any other document, it is because I have approved or agreed with the contents of that document and, in a commercial context, have accepted the legal consequences that flow therefrom. If the document is unclear or if I do not understand the contents, then that is a problem unrelated to the form my signature takes. In my view, legislation of the type under consideration should not be used to protect the careless, unwary, reckless or infirm from the consequences of their actions.

Summary

Electronic messages are not the same as paper documents, electronic signatures are not the same as handwritten signatures and no amount of legislative legerdemain can make them the same. However, I believe that legislation can be enacted which would make electronic and Pen Signatures functionally equivalent, provided that there is clarity as to the function or functions which are to be equivalent. The Model Law suggests three functions of Pen Signatures and I have taken issue with two of them, suggesting instead that the sole function of universal application is to provide evidence of an association between a person and a document.

I have suggested that the nature of the association between a signer and a document has to be ascertainable from the document itself. If I don't agree or approve of a document, then I don't sign it. If part of the document is not applicable to me (eg. if I sign only as a witness to one party's signature), my signature is not evidence of my approval of or agreement with that part. The Model Law requirement that an electronic signature indicate approval of the information contained in the document is too inflexible and, in the case of digital signatures, unworkable.

The Model Law provides for recognition of electronic signatures under certain conditions where a signature is required by law or if there are consequences arising from the lack of a signature. Presumably, the argument is: If the law doesn't require a signature, then the existence of one is not relevant. I have not touched on conflict of laws issues in this paper, and there may be cases where, in a cross-border transaction, one jurisdiction clearly requires a signature and the other does not. The point I want to make is simply that, in many cases it is not clear whether the law requires a signature. If it is clear by statute that a signature is required, then the process for electronically signing a document should be similarly clear and recognition should follow if the process is observed. If the law does not necessarily require a signature, then legal recognition of the signature should not necessarily follow, rather the legislation should simply provide that the signature not be denied legal effect solely because it is not a Pen Signature. To provide a presumption as to validity for, for example, secure electronic signatures, would be to create a new animal with different functionality from Pen Signatures and would disturb an established, and substantive, rule governing the burden of proof.

There may currently be no impediment to using electronic signatures (other than in what I have called Category A cases, where a signature is required by statute), but to remove any doubt, I would encourage legislation to that effect.

I have invited readers to consider whether any issues arise because of the difficulty of separating "execution" from "delivery" in electronic messages. That is, after sending an electronically signed document, whether by fax, email, digital signature or whatever technology may be used, it is "out there". Whatever control we may have over the delivery of paper documents does not exist or is, at least, limited, in the case of electronic documents.

The Model Law proposes that an electronic signature reliably identify the signer. I have suggested that the identity of the signer may or may not be relevant. Instead, one or more attributes of the signer (which could include his, her or its identity) are what are really being linked to the document by a signature. Recall my example of "over 18 years old-ness" and "not residing in Alabama-ness."

Proof of the relevant attributes of an electronic signer should be left to the parties to an electronic transaction, in the same way that proof of a Pen Signature is a matter for the recipient to seek. In the example of the vendor of dirty pictures on the internet, he may very well insist that his customers obtain a particular grade of certificate from a particular CA (assuming that a "due diligence" defence exists to whatever offences he may inadvertently commit) or he could rely on nothing more than an email message.

Lest anyone feel that I am in favour of a "buyer beware" jungle on the internet, I am not. I am simply suggesting that, for example, fraud on the internet is fraud and should be dealt with, not in legislation removing real or perceived barriers to electronic commerce, but in legislation dealing specifically with preventing fraud.

The Model Law requires that an electronic signature indicate the signer's approval of the contents of a data message. While approval of something relating to the document is likely a universal purpose of a signature, that approval has to be tied to the particular signer. An electronic notary is not approving the terms of an electronic contract, he or she is simply providing some assurance that is was signed by a particular person.

July 1998