Canadian and American Legislation on Electronic Signatures with reflections on the European Union Directive

John D. Gregory

The earliest legal concerns about electronic transactions have generally arisen from form requirements, or what could be called “medium” requirements, i.e. (apparent) requirements that a particular medium of communication be used for legal effect. The law often demands or presumes the presence of paper. What happens when one takes the paper away? This article considers first the general nature of law reform in electronic commerce, then the nature of signatures, then at how laws in Canada and the United States have handled the question of signatures in paperless transactions, with an eye on European Union parallels.

It is important to appreciate the border between legal requirements and prudent business practice. Many transactions are conducted with paper documents not because the law makes people do it that way but because people are accustomed to do it that way, or because it makes sense to do it that way, or because it’s easier to prove that way. The letter X in pencil on a document is capable in law of constituting a signature. Nevertheless most people would not accept a cheque signed only with an X. Where a medium is chosen for prudence and not to satisfy legal requirements, the parties are generally free to choose an electronic medium instead of paper. The concern at that point is to judge the reliability of the electronic documents (as well as their provability.) Most of us do this with less confidence than with paper documents, since we draw on centuries of experience in knowing what to do with writing on paper.

II. APPROACHES TO ELECTRONIC SIGNATURE LEGISLATION

Two approaches have been taken to supporting the reliability of electronic documents so they can be accepted in law. The first is to indicate only the general nature of the results to be achieved in using electronic documents, leaving the details to the parties and the circumstances. The second is to spell out in detail the technology or at least how the technology is to work to create legal effects. Both approaches have been tried in electronic signature legislation, and indeed some such legislation has combined both for different kinds of signature.

It is fair to say that in North America, the first approach has gained more ground

than the first. Minimalist, technology-neutral legislation has generally been used to deal with electronic documents and signatures. Early attempts at technology-specific statutes have generally not found successors, though they have influenced some hybrid legislation. There is a limit to how much the law can help settle questions of trustworthy practice, and a limit to how much the law should try to do so.

A. Minimalist Legislation

1. Reasons for minimalism

Both Canada and the United States have generally preferred a minimalist response to the quest for certainty about the legal status of electronic communications and electronic signatures. It is minimalist for several reasons. First, the existing law – statutes and common law and private law based on contracts – is capable of resolving a good number of questions on its own. Electronic messages, even on the Internet, do not present radically new questions in every field. Next, the technology underlying electronic records is changing rapidly, so attempts to prescribe specifically how to conduct legally effective communications risk obsolescence even before they come into force. In any event the uses to which electronic communications are put vary so widely that no single technology would suit all of them. The statutes can be said to be "technology neutral" for this reason. Finally, e-commerce is global in scope, and neither country wants to take a seriously different approach from its major partners. The international consensus today is arguably in favour of minimalism, as shown by the success of the U.N. Model Law on Electronic Commerce. Many countries have enacted laws based on the U.N. Model Law.

Minimalism has been particularly attractive in Canada and the United States for dealing with signatures. The basic function of a signature is to link a person with a text or document. Thus a signature must identify or permit the identification of a person (which may be a natural or legal person), possibly along with other evidence of identity. In other words, a signature is evidence of attribution of the text. The signature may be made by the person or by someone acting for the person. It may be written by hand or made by some mechanical means. On paper, of course, the signature generally appears in the same physical document as the text.

It is important to note that nothing in the form of the signature itself shows the intent with which it was made or the purpose for which it appears. The intent or purpose may be inferred only from the context, i.e. from the signed document. Sometimes this is easy: a signature at the end of a contract may readily be inferred to indicate an agreement to be bound by the contract. However, move that same signature to the top of the contract and its intention is much less clear. Put it on the back of the page and the intention may be very obscure. So the rest of the document shows the legal effect to be given to the document signed by the identified person. The content of the document, and thus context for the signature, is more important than the physical characteristics of the signature itself.

In these circumstances it is arguable that an electronic signature qualifies as a signature without any legislative assistance. An electronic signature can identify or permit the identification of a person and it can be part of or be linked to a text, the context of which will show its purpose. Why then have almost all jurisdictions in Canada and the United States legislated on electronic signatures? In part, legislators have wanted to create certainty that e-signatures would be accepted despite their novelty. Some kinds of legislation attempt to set out the duties of parties to electronic signatures in a manner intended to reduce perceived risks of such signatures and thus to promote electronic commerce. Some

places have adopted comprehensive legislation based on models that included provisions on signatures. In addition, signatures are an important symbolic part of a transaction, the part that symbolizes the binding of the signer, the human and ceremonial touch. It was hard to leave this out of legislation dealing with electronic communications in general.

2. The American and Canadian uniform legislation

The American uniform statute based on the U.N. Model Law on Electronic Commerce is the Uniform Electronic Transactions Act (UETA), adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in July, 1999. To put the U.N. Model Law into Canadian statutory language, the Uniform Law Conference of Canada adopted the Uniform Electronic Commerce Act (UECA) as of September 30, 1999, and recommended it for adoption by the member jurisdictions of the Conference – all the provinces and territories of Canada and the federal government. Both statutes affect more than commerce; the UETA covers "transactions" and the UECA "information", subject to express exclusions.

Neither the Model Law on Electronic Commerce nor the two uniform statutes intend to change the substance of the existing law. They intend only to make the law media neutral, equally applicable to paper and to electronic documents. The treatment of "electronic signature" therefore does not create a new legal "thing" with this name. Rather it deals with the essential functions of any signature. The Canadian definition reads, "'Electronic signature' means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document." The American definition is, "an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." The legal essence of a signature is the intention with which it was made, rather than its form or medium. The intention in both statutes is "to sign". The use of the word "sign" was deliberate. The existing law about the appropriate intention for an effective signature, and how one proves it, continues in effect. (The definition in the EU Directive on Electronic Signatures is about the same, except that it uses the more obscure synonym "authenticate" for "sign".)

The purpose of defining electronic signature is to make clear that the electronic version does not have to look like a handwritten signature when it is displayed. It may be code or sound or symbol of any kind, if the intention is present. Likewise, an electronic signature may travel apart from the document it signs, if the association with the document is clear. In fact, the wording of the definitions would allow the use of an electronic signature to sign a document on paper.

The UECA and the UETA provide that a signature requirement can be met by an electronic signature. Unlike the U.N. Model Law, they do not go on to require that the electronic signature must be as reliable as is appropriate in the circumstances. At common law, and arguably in the civil law of Quebec as well, a method of signature on paper does not have to meet any test of reliability. If the association with a person is demonstrated and the intent to sign is demonstrated, the signature will meet the signature requirement. Those elements will have to be shown in order to meet the definition of electronic signature. The Uniform Acts are not trying to make the law better, just neutral. The EU Directive imposes no general requirement of reliability but leaves proof to the parties.

However, it is possible that the authority that imposed the signature requirement in the first place did have some degree of reliability in mind. In that case, the UECA allows that authority to make a regulation imposing the reliability standards of the U.N. Model Law.

3. Non-uniform minimalist statutes

a. E-Sign

Besides the uniform statutes, both the United States and Canada offer another significant example of a technology-neutral electronic signature law. The American example is the federal statute, the Electronic Signatures in Global and National Commerce Act, known popularly as "E-Sign." E-Sign was inspired by the Model Law and by UETA, but was intended to harmonize the law across the country for interstate commerce, a concept that covers a lot of activity in the United States. While UETA does not impose additional requirements on electronic signatures, E-Sign does limit its application in respect of several kinds of consumer transaction. Otherwise E-Sign prohibits state legislatures from enacting any rules for electronic signatures that would be more onerous, or more technology-specific, than the rules of the UETA, of which E-Sign encourages the adoption.

b. Quebec's legislation

The additional Canadian legislation in this category is Quebec's Act to provide a legal framework for information technology. It aims to make the law almost completely media-neutral, and spells out ways by which rules of law can be met by intangible information. The stability of the content of the document is a primary concern of the Act. It is arguable that parties to electronic transactions governed by statutes implementing the Uniform Act will have to be sensitive to the same concerns as those stated in the Quebec Act. Quebec does not leave the resolution of these concerns quite so much to the education or sophistication of the parties as does the Uniform Act, though both statutes leave open the means of achieving the appropriate degrees of assurance.

While this statute is technology neutral, it spells out in much more detail the requirements for appropriate attribution of what it calls "technology-based documents". Signatures are just one form of evidence of attribution in this statute, a point in which it joins the analysis made earlier for the common law. Section 38 of the Act says that a link between a person and a technology-based document may be established by any process that allows the identity of the person to be confirmed and the link with the document to be confirmed, and of course the document itself to be identified. Section 39 provides that a signature may be used to establish this link, and refers back to article 2827 of the Civil Code for what constitutes a signature. In short, the Act, though in different language, has the same effect as the UECA: it allows new technology to create a signature but leaves the essence of a signature in law the same as it was for a signature on paper.

4. Prudence and Consent

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

This need for the parties to decide what they need for their own purposes makes the consent rule absolutely fundamental in both these technology-neutral statutes. Only the proposed user can make that judgment for his or her own purposes. The power to

say No is the power to say Yes, if … the signature is secure enough, or satisfies other concerns of the recipient. It is also important to note that the consent is not necessarily comprehensive. One may accept some kinds of information in electronic form and reject others, or accept it for some purposes, or accept electronic documents but not electronic signatures.

As a result of the consent provision, the fact that an electronic signature satisfies the legal requirement for a signature does not make that signature effective against someone who does not want to deal electronically at all. Since most electronic communications, and certainly most commercial transactions, will be on consent, this will not usually be a problem. Both statutes say clearly that consent to use electronic documents may be inferred from conduct, moreover; an express agreement is not needed. Otherwise there is too much risk of bad faith refusal. In addition, people may bind themselves by contract to accept electronic signatures, and other law – including for example employment law – may compel them to do so. Questions arise about how much consent is needed and how broad it may be. If one puts an e-mail address on a business card, has one consented to deal electronically for all purposes?

5. Attribution of documents and signatures

Article 13 of the U.N. Model Law on Electronic Commerce provides that data messages may be attributed to those who create them or who authorize their creation. This is of course the general law in Canada and the United States. The UETA has a similar provision. The Canadian Conference thought this went without saying, so did not say it.

The 1996 U.N. Model Law goes on to provide a rule of attribution where certain agreed security procedures are used on data messages. NCCUSL attempted to devise similar rules, but they fell under severe criticism based partly on the fluidity of the technology available and partly on the likely lack of sophistication of its users. The Canadian Conference did not try to follow the Model Law on this point in the Uniform Act, but the federal government has given it some echo in its legislation, discussed below. The working group of UNCITRAL on electronic signatures aimed to give more substance to the provisions of Article 13 of the 1996 text, but there too, efforts to draft clear attribution rules ended up much narrower than originally hoped.

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

B. Non-minimalist statutes

1. Reasons for a more detailed approach

The other major approach to electronic signature legislation is to spell out the requirements for such signatures in more detail. There are two main reasons for taking this approach. First, people are concerned about the reliability of electronic documents, including signatures. It is easy to amend many electronic documents, and the amendments may be very hard to detect. More rules are thus thought to be needed to ensure that electronic information that will constitute a signature is appropriately secure.

The second reason for taking a more detailed legislative approach is that the nature of electronic signatures is often different from that of signatures on paper. A signature on paper involves two people or classes of people: the signer and the person(s) who rel(y)ies on the signature. While an electronic signature may also involve only the same two classes, it may also involve a third person, someone who acts as an intermediary to establish the relying party's trust in the signature itself. An electronic signature is only bits, like any other electronic document. Many people believe that e-signatures will inspire more confidence if a trusted third party certifies to the relying party that the signature bits are in fact the signature of a particular person. Legislation has thus been devised to ensure that such certification authorities (CAs) follow trustworthy procedures. Some of them offer limitation of liability for mistakes of identity if the proper procedures are followed, and some offer to the relying party reinforced credibility of the identification in such certificates, by way of a presumption of attribution.

2. Technology-specific legislation

Much of the early conceptual work about such a system was carried out by the American Bar Association, whose Digital Signature Guidelines were influential. The first legislation to this effect was the Utah Digital Signature Act of 1995. It dealt expressly with public key cryptography as signature. It regulated CAs and exempted them from liability if they followed the rules. It also provides a presumption of attribution for duly certified signatures. The Utah Act was followed in three other states.

However, this approach was severely criticized on several grounds. First, it was said to distort the true value of the technology to legislate liability. Essentially the statutes were allocating risk by law differently than how the real risk fell. This was "legislating market winners", which was said to be inappropriate in a free market. Second, as technology evolved there were many different implementations of digital signatures, with different degrees of involvement and engagement by CA s and relying parties and thus different risks. Third, digital signature legislation was thought to impede the free development of signature technology, as it gave an unfair legal advantage to the technology of public key cryptography. In the result, no furher states have followed the Utah example.

3. Technology-neutral hybrid statutes

a. American hybrid legislation

As the Utah model fell into question, attempts were made to find technology-neutral statutes that would nevertheless recognize that some kinds of e-signatures were more reliable than others. The most solidly drafted of these was the Illinois Electronic Commerce and Security Act of 1998, which went through several public drafts with commentary on its way to passage. Illinois provided that parties might agree that an electronic signature would satisfy a legal signature requirement. In addition, particularly reliable e-signatures were described as "secure electronic signatures". These had certain characteristics first described in the United States by the National Institute of Science and Technology (NIST) in the early 1990s.

These characteristics were, in the words of the Illinois Act:

- The signature is unique to signer in the context in which it is used;
- It can be used to objectively identify the person signing the electronic record;
- It was reliably created by such identified person (e.g. because some aspect of the procedure involves the use of a signature device or other means or method that is within the sole control of such person) and that cannot be readily

duplicated or compromised;
- It is created and linked to the electronic record to which it relates, in a manner such that if the record or signature is intentionally or unintentionally changed after signing then the electronic signature is invalidated.

Illinois allowed the Secretary of State to designate electronic signature systems that met these

criteria, so that litigants would not have to prove compliance with them in every case. Where the criteria were present, the Act provided a presumption of attribution, i.e. that the signature actually came from the person who apparently made it. It also sets out criteria for evaluating the reliability of certificates.

The Illinois model has influenced many others, including California in the US, Singapore (the first nation to implement the U.N. Model Law on Electronic Commerce), the UNCITRAL Model Law on Electronic Signatures and the European Directive on that subject.

b. Canadian hybrid legislation

In Canada, the federal government has adopted its own form of legislation: the Personal Information Protection and Electronic Documents Act (PIPEDA), Part 2 of which deals with electronic documents. It is a hybrid statute as well. Some of the signature provisions simply allow signature requirements to be satisfied electronically by use of an e-signature in the form to be prescribed by regulation. However, several sections contemplate the use of a "secure electronic signature". For example, one can use a secure electronic signature to create a certificate signed by a minister or public official that is proof of a fact or admissible in evidence. A secure electronic signature may serve as a seal, if the seal requirement has been designated under the Act. Affidavits may be made electronically if both deponent and commissioner of the oath sign with a secure electronic signature. Declarations of truth may be made with such signatures, in similar circumstances. Witnesses may sign under similar conditions. It is worth noting that unlike the Illinois hybrid, the federal statute gives no choice about whether to use a secure electronic signature. To sign electronically and validly within the meaning of the provisions named, people must use the secure electronic signature.

A "secure electronic signature" is not defined in the Bill, except as "an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1)". That subsection sets out the usual provisions for signatures of this type, as we have discussed above in regards to Illinois. The intention is that in the first instance the only technology to be designated will be that of digital signatures certified by the Government of Canada, or those from systems cross-certified with the GOC PKI. Some provincial governments are developing public key infrastructures as well, and they hope to be cross-certified with the federal PKI. To date no regulations have been made on secure electronic signatures.

As noted earlier, Manitoba also uses the concept of secure electronic signatures, and Prince Edward Island uses the NIST list in its general definition of electronic signatures. It is too early to tell what impact their provisions will have on electronic transactions governed by them.

The Quebec statute mentioned in the first section as a technology-neutral statute nevertheless makes detailed provision for the activity of persons who certify the identity of signatories of technology-based documents and it sets up a voluntary

accreditation scheme for them. It also examines the nature of recognized standards for reliable technology in this area. Further, Quebec provides for the liability, or the exemption from liability, of communications intermediaries like Internet service providers.

c. International hybrid legislation

The UNCITRAL Model Law on Electronic Signatures aims to help the parties determine in advance whether the reliability standard of the 1996 Model Law has been met. The new Model Law also avoids detailed descriptions of the technology to be used, however, for the reasons that support minimalism in the first place. Earlier drafts talked of "secure" or "enhanced" electronic signatures. The terms have been dropped but the criteria of identification, sole control and detection of alteration remain in the new criteria for reliability of an electronic signature.

Compare the European Union's Directive on Electronic Signatures. It ensures that electronic signatures can be valid despite their electronic form and despite not meeting the more demanding standards described in the rest of the Directive. It goes on to prescribe in considerable detail a regime for "advanced electronic signatures" created by a "secure-signature- creation device" and supported by "qualified certificates". Again one recognizes the NIST/Illinois language, though the appendices on technical requirements for qualification are more detailed than in those texts. The result of using this technology is an electronic signature to which member states must give the legal effect of a handwritten signature. There are no presumptions of attribution. This may strike some as a weak result for a strong technology.

These detailed requirements will not be easy to meet, judging from the difficulties in setting up public key infrastructures in Canada and the United States. However, even when they are, the assurances of identity of the signatory are vulnerable, depending on the design of the system. As noted in the earlier discussion of the nature of a signature, the fact of a signature is less valuable in a commercial transaction than evidence of attribution. (Indeed, the identity of the other party is often less important than its solvency or the quality of its goods or services.) Business parties may in practice choose to satisfy themselves about attribution through procedures that do not qualify as a signature at all, and certainly not as an advanced signature.

The Directive contains as well provisions on the liability of parties to signatures, on recognition of foreign signatures and certificates, and on respect of privacy rights. The first two items were clearly inspired by the parallel discussions on these topics at UNCITRAL, as were some of the criteria for qualified matters in the appendices to the Directive. In the legislation in the United States, only Utah and its followers dealt with liability, and then to exempt regulated certification authorities from liability if they followed the rules. Some of the requirements for qualification have echoes from Illinois. In Canada, Quebec's statute has provided rules on liability and data protection similar to those of the Directive. Otherwise the minimalist statutes leave these topics for another day.

III. RELATED TOPICS

A. A Note on Evidence

In general the common law does not give signatures or signed documents any special status as evidence, except for documents signed by public officials which may be "self-authenticating", i.e. admitted without proof of origin beyond that signature. As a result, most of the U.S. and Canadian statutes discussed here say

very little or nothing about evidence questions.

The UECA is silent on evidence. The Uniform Law Conference has adopted a separate statute on electronic evidence, but it too says nothing about signatures. The UETA says only that evidence of a record or signature may not be excluded solely because it is in electronic form. E-Sign is silent as well on evidence. Many of the uses of secure electronic signatures in the Canadian federal legislation support an evidentiary use, however. The Canadian federal legislation amended the Canada Evidence Act to allow the creation by regulation of presumptions of the association of secure electronic signatures with persons, and of the integrity of information in documents where a secure electronic signature is used. No such regulations have been made to date.

In Quebec, as noted earlier, an electronic signature is approved where made "by means of any process that meets the requirements of article 2827 of the Civil Code", which is part of Book VII of the Code on evidence. No special rule of admissibility is provided. The Quebec statute did amend one article of the Civil Code on the use of electronic documents as evidence, without mentioning signatures in particular.

By contrast, the EU Directive on Electronic Signatures provides that qualified electronic signatures must be admissible in evidence, and that other electronic signatures may not be denied admissibility on grounds of their electronic form or because they are not qualified in one element or another. To the extent that documents are more readily admissible when signed, and that courts will be hard to satisfy in practice with less than an advanced signature, compliance with the requirements for an advanced signature would be more important in European law than in Canadian or American jurisdictions.

B. A Note on Standards

The choices for private parties and public parties may be made easier by the development of technical standards for the use and admissibility of electronic signatures. Such standards are being worked on domestically and by international organizations like the International Standards Organization, and within Europe by the European Electronic Signature Standard Initiative. This could be compared to the work of the American Bar Association on evaluating public key infrastructure programs, recently published for consultation. Compatible technical standards are the likely underpinning for mutual recognition of certificates and thus electronic signatures.

The impact of the standards on practices and thus on the need for legislation in the future remains to be seen, and will no doubt furnish the material for another article.

IV. CONCLUSION

The main legislative approach to electronic signatures in the United States and Canada is minimalist and technology neutral. This approach puts a lot of responsibility on the parties to a signature, particularly on the relying party, to decide what kinds of electronic signatures they will accept for what purposes. The risk of loss from a fraudulent signature remains on the relying party, as it is for signatures on paper.

The major exception to this approach is essentially public sector electronic signatures. Many levels of government are developing digital signature systems supported by certificates to be used in dealings between citizens and the government. To date only the Canadian federal government has legislated expressly on that front, though with concepts taken from Illinois and elsewhere. Other jurisdictions are contemplating whether to legislate to support the reliability of

their public key infrastructures, or to set out the duties and liabilities of the parties to certified electronic signatures. The UNCITRAL Model Law on Electronic Signatures and the EU Directive contribute to that process of reflection.