ARTICLE:

MUST E-SIGNATURES BE RELIABLE?

By **John D. Gregory**

This note criticizes the statutory requirement that the validity of an electronic signature depends on its being as reliable as appropriate in the circumstances. This requirement unfairly discriminates against electronic signatures (having no equivalent for signatures on paper). Common law does not impose any form requirements on what can be a signature, so no statutory standard is needed to support an e-signature. The law should not impose a standard of prudence that must vary among transactions and among parties to them. Finally, the reliability standard risks invalidating e-signatures that are demonstrably genuine. Neither consumer protection nor high security needs justify the generic reliability rule.

The United Nations Model Law on Electronic Commerce of 1996,[1] the basis for the laws on electronic transactions in many countries around the world, provides that when the law requires a signature, the requirement may be met by a method that identifies the person who is supposed to sign, indicates his or her approval of the information, and '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.'[2]

I am very sceptical of any legal requirement that electronic signatures must be as reliable as appropriate in the circumstances. We thought of using such a requirement when we drafted the Uniform Electronic Commerce Act[3] in Canada, and decided against it. The official commentary on the Uniform Act says this:

> Although the UN Model Law makes an electronic signature meet a test of appropriate reliability in order to meet a signature requirement, the Uniform Law Conference felt that such a test would detract from the "media neutrality" of the Uniform Act. However, where the authorities responsible for a signature requirement take the view that the requirement does imply some degree of reliability of identification or of association with the document to be signed, they may under subsection (2) make a regulation to impose a reliability standard. The language of subsection (2) is based on that in the Model Law.[4]

All of the common law provinces and all the territories have implemented the Uniform Act and all but two have maintained the open-ended provision of that Act. None has made a regulation of the kind described in the annotation. Manitoba[5] requires reliability for an electronic signature on 'a document of a prescribed class', though none seems to have been prescribed yet. Prince Edward Island[6] has a definition of 'electronic signature' derived from the UN Model Law on Electronic Signatures, though its parliamentary debates give no reasons for this deviation from the Uniform Act, otherwise closely adhered to, and no courts appear to have been called on to interpret the provision.

The first reason for not having a reliability rule is that there is no such rule for handwritten signatures (or any of the other marks on paper that may constitute a signature at law). The person relying on a signature always takes the risk that the signature is not genuine, so he or she acts accordingly. That is to say, the relying party evaluates the risk that the signature is not genuine and protects himself or herself or itself accordingly. This may involve checking the signature against known genuine versions of it, or getting the signature witnessed, or getting the signature notarized, or getting the signature guaranteed by a bank, or various other techniques. The risk analysis will of course include the cost of having the signature made more reliable and the cost of its being not genuine. So a course of dealings with the purported signer, or a low-value transaction, may persuade someone to rely on a signature that from a stranger or for a high value would not be satisfactory.

1 *United Nations Model Law on Electronic Commerce, 1996, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.*
2 *UN Model Law on Electronic Commerce, above, note 1, article 7.*
3 *Uniform Electronic Commerce Act, http://www.ulcc.ca/en/older-uniform-acts/electronic-commerce/1650-electronic-commerce-act-annotated-1999.*
4 *Uniform Electronic Commerce Act, above, note 3, commentary to section 10.*
5 *Electronic Commerce and Information Act, CCSM c E55, s. 13, http://www.canlii.org/en/mb/laws/stat/ccsm-c-e55/latest/ccsm-c-e55.html.*
6 *Electronic Commerce Act, RSPEI 1988 c E-41, s. 1(b), http://www.canlii.org/en/pe/laws/stat/rspei-1988-c-e-4.1/latest/rspei-1988-c-e-4.1.html.*

These precautions and judgments are not a matter of law but a matter of prudence. The law applicable to electronic signatures can be the same.

Second, the common law does not impose any form requirement on signatures – which means it is arguable that an electronic signature is a good signature without any law reform.[7] At common law, I can sign something by authorizing someone else to sign my name – meaning that a handwritten signature may not look like what I would write but is mine and enforceable against me nonetheless. (There are questions of proof in all of this – and so there are in e-signature questions – but they should not distort the law on the point.) Likewise I can sign by machine (with the same practical questions). If I can sign by a machine that prints my name – possibly but not necessarily in the form of my handwritten signature – then why should I not sign with a machine that creates electrons that link me with the text?

The basic – arguably the only – common function of a signature is to link a person (i.e. legal entity) with a document.[8] Nothing in the form of the signature states the legal effect of that link. One cannot know the link without knowing the context – starting with the obvious question what the document is that bears the signature (or to which the signature relates). The context will always have to be demonstrated, whether on paper or electronic. Sometimes that will be hard, most of the time it will be easy.

But the important point remains: it is not the form of the signature that gives it any legal effect. Therefore any information in any medium that is capable of linking a legal entity with a document (electronic or paper or other) should be able to be a signature at law.

There is a mental element in a signature: the person must have an intention to sign the document, though the reason for the intention may vary.[9] The Uniform Electronic Commerce Act defined an electronic signature by saying it was 'created or adopted in order to sign a document'.[10] In other words, it incorporated the same mental element for e-signatures that the (common) law requires for all signatures. It made no legal distinction between the purpose or intention of an e-signature and those of a signature on paper. That mental element will be shown, once again, by the context (such as text saying 'signed by') rather than by use of a particular technique or technology. The reliability of the context to do this can be shown for electronic signatures as it can be for handwritten or otherwise mechanically produced signatures, without a special statutory rule.

Third, in my view law reform should not restrict this flexibility of the common law. There are many examples where the law will give effect to practices that may not be prudent for people to engage in. People are expected to be prudent. An 'X' in pencil on a piece of disposable tissue paper can be a legally effective signature, but most people would not accept a valuable contract made on such a medium with such a signature, because the risks are too great.

Part of the challenge is that people have many years of experience in evaluating how reliable a signature on paper is, and thus can judge what is prudent. People are much less familiar with the potentials and vulnerabilities of methods of signing electronically. However, I would submit that the law does not add any value to this lack of familiarity with an 'appropriate reliability' test. Such a test merely transfers the prudential judgment from the relying party to a judge – who may be no more competent to make it, though he or she may have the advantage of expert evidence. It may be a complicated decision. The Guide to Enactment of the Model Law on E-Commerce sets out fourteen different considerations for 'the circumstances' in which a signing method is to be judged reliable.[11] Such considerations are also available to the relying party – at a more useful time, before the transaction is consummated.

The Federal Court of Australia decided in G*etup Ltd v Electronic Commissioner*[12] that indeed the entity to which the e-signature was submitted, and which was intended to rely on it, did not have the power to determine its reliability. Only the court could do this. In other words, the parties to a communication using an electronic signature are always subject to having their choices held invalid by a court – or in the *Getup* case, held valid though the party intended to rely on it did not think it was sufficiently reliable for its purposes. Either way, this seems undesirable. (In common-law Canada, the *Getup* decision would have gone the other way, both because the applicable statutes do not compel anyone to accept an electronic communication – as discussed in more detail below – and because a government or public

7 *The Law Commission of England and Wales came to that conclusion in 2001, paragraphs 3.42 – 43, http://lawcommission.justice.gov.uk/docs/Electronic_Commerce_Advice_Paper.pdf.*

8 *Chris Reed, ' What is a Signature?' , 2000(3) The Journal of Information, Law and Technology, 3.1.1, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.*

9 *The Guide to Enactment to the UN Model Law on Electronic Commerce gave seven different kinds of intention that might be associated with a signature – a non-exhaustive list. Guide to Enactment, paragraph 53.*

10 *Uniform Electronic Commerce Act, above, note 3, s. 1.*

11 *UN Model Law on Electronic Commerce, Guide to Enactment, paragraph 58.*

12 *[2010] FCA 869.*

body may in addition impose its information technology requirements on any incoming e-document or e-signature, to ensure compatibility with its systems and its judgment of reliability.[13])

Fourth, a reliability requirement risks becoming a trap for the unwary, or a potential loophole for the unscrupulous. One can readily imagine a situation where the relying party knows the person who created an electronic signature and there is no question about the link to a document – yet tries to avoid an agreement by saying 'yes, I know all that, but the method of the e-signature was not reliable enough for this transaction, so the signature, and thus the transaction, cannot be valid.' The person who created the signature cannot know at the time of creating it – at the time of the e-transaction that the 'enabling' legislation is intended to facilitate – whether a court will hold it to be appropriately reliable. The other party can argue it is not that reliable, in bad faith, possibly. For that matter, the person creating the signature might use the same argument: 'Yes, I signed it, but it did not meet the legal test for validity.'

Probably most court systems would resist allowing either of the parties to a signed document to use this kind of argument to invalidate a transaction they participated in. The more substantial risk is an attack on that ground by a third party, someone not involved in the transaction but who has a motive to invalidate it. One thinks of tax authorities, trustees in bankruptcy, possibly even ex-spouses, who would like to see assets owned by one party and not by another. Because of the complexity of the evaluation, as noted above, a judge could readily come to a different conclusion than the parties on the reliability question. It is not clear what public interest is served by such a result.

In short, the reliability test does not deal with what parties should reasonably be expected to ascertain – who signed what for what purpose? It adds an unforeseeable element, an optional escape method, for attacking a signature with respect to which all relevant questions are answered. And it does not help answer any of those questions independently.

I would also submit that the list of tests in the Model Law on Electronic Signatures[14] (article 6(3)) adds little of real value as well, but that is a whole different set of arguments. It would often if not usually be harder to prove compliance with the technical standard than to authenticate the document directly.

It is worth noting that the UN Convention on the Use of Electronic Communications in International Contracts,[15] adopted in 2005, expanded on the grounds for validity of electronic signatures. Besides the reliability test, which was vigorously contested at the meeting where the Convention was adopted,[16] the Convention allows for validity of a method of identifying a person and indicating the person's intention in respect of information if the method is 'proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.'[17] Authentication in practice, not just in principle, can be effective in law.

Is consumer protection an exception to my argument against a reliability test, since consumers may be even less able to judge prudence of accepting an e-signature than a commercial party? I doubt that consumers would be helped by an open-ended reliability requirement either. They too can be trapped by it. Consumers probably need to know identity more than they need to see a signature as such demonstrated. So consumer protection in e-commerce should depend more on enforcing full disclosure of identity, place of business, and rights and remedies for the transaction than the artificial and generally irrelevant consideration of the form of a signature.[18]

All this discussion assumes that there actually are rules of law that require a signature, since if there are not, the enabling legislation based on the Model Laws does not apply at all. It does not apply to support or weaken a signature on a private transaction not covered by any statutory requirement. All the more reason not to have any unpredictable technical demands. In the few cases when the issue may come up, the parties will be even less expecting such a strange loophole.[19]

One way the Uniform Act in Canada leaves reliability

13 *See for example the Uniform Electronic Commerce Act, section 10(3).*

14 *United Nations Model Law on Electronic Signatures http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.*

15 *The 'Electronic Communications Convention' http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.*

16 *Report of the UNCITRAL meeting of July 2005, A/60/17, paragraphs 65 – 68 http://www.uncitral.org/uncitral/en/commission/sessions/38th.html.*

17 *Electronic Communications Convention, article 9(3)(b)(ii). See also the Explanatory Note on this clause published by UNCITRAL, http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf at paragraph 164.*

18 *For one system of consumer protection in online sales among many in the world, consider Canada's Internet Sales Harmonization Template, in force in most provinces, http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca01642.html.*

19 *This note focuses on signatures, not on authentication generally. A signature is only one method of authentication. Just as the relying party can decide whether to rely on a signature, he/she/it can decide to rely on a document with no signature (unless the law requires one). No one, however, would rely on a document that they believed to be inauthentic, or about whose origin they had no idea.*

to the parties is its consent rule. It says that nothing in the Act requires any person to use or accept information in electronic form.[20] If one can refuse an electronic document, or an electronic signature, then one can accept it if it is sufficiently reliable – not in some abstract sense, not in a way determined by a judge two years later, but at the time of use. The consent rule, in other words, gives the potential relying party a clear opportunity to decide if the electronic signing method is satisfactory to it. If not, the party can insist on paper documentation.

There may be a case for spelling out more detailed requirements where signatures must be more reliable than usual, or where the decision on reliability should not be left to the immediate parties to the documents. This additional caution applies to handwritten signatures as well. Common law jurisdictions often provide, for example, that wills requires two signatures of witnesses both present at the same time and signing at the same time. Canada's statutes to this effect are excluded from our electronic commerce statutes.[21] In any event, a generic reliability test adds little protection to such circumstances. In cases needing extra security, one would arguably want to be less technology neutral and more prescriptive. Another Canadian example: Ontario's electronic system for registering land transfers,[22] depends on a thoroughly prescribed network of digital signatures and identities certified by the Law Society.

None of this justifies restricting people signing normal documents electronically to a standard of reliability that is unsound in theory and misleading or even dangerous in practice.

John D. Gregory is General Counsel, Justice Policy Development Branch, Ministry of the Attorney General, Ontario, Canada. He chaired the working groups that created the Uniform Electronic Commerce Act and the Uniform Electronic Evidence Act, and has been on the Canadian delegation to the UNCITRAL Working Group on Electronic Commerce since 1997. The views expressed in this article are not necessarily those of the Ministry.

20 Uniform Electronic Commerce Act, section 6.

21 Uniform Electronic Commerce Act, section 2(3)(a). However, when the Uniform Law Conference revisited the question of electronic wills a few years later, it thought that there was a case for allowing them. In any event, laws validating wills 'in substantial compliance' with statutory form requirements would probably accept wills in electronic form, http://www.ulcc.ca/en/2002-yellowknife-nt/306-civil-section-documents/124-recognition-of-wills-and-powers-of-attorney-in-electronic-format-2002.

22 The system is described in general terms here: http://www.gov.on.ca/en/information_bundle/land_registration/content/STEL02_165314.html.

