Toronto Law Journal

Electronic Signatures in Ontario Law

John D. Gregory[1]

If one looks hard enough for some good news relating to the pandemic of 2020-2021, it could include the widespread adoption of electronic signatures. Having to avoid meetings in person has pushed lawyers and clients into remote transactions, authentication, and notarization. One might think it was about time. This short article addresses the nature of signatures, the law applicable to electronic signatures, and some technical and practical considerations of using them.

Signatures

A signature is a method of linking a legal entity (individual, corporation, government) to a known text.[2] The purpose of the link can vary. It includes consent, witnessing, acknowledgement, and transfer. Nothing in the law says how this link is to be created or evidenced. Moreover, nothing in the form of a signature shows its legal purpose. The signatory's intention must be taken from the context.

Traditionally, of course, signing has been done by handwritten ink on paper; handing over clods of earth or affixing personal wax seals both fell out of fashion centuries ago.[3] Ink on paper has for a long time been the most convenient form of producing evidence of (or "authenticating") the link. However, these functions can also be performed electronically.

Thinking about signatures in electronic form makes us focus on the essential elements. Many courts have tended to assume things that are not accurate, *e.g.* that the signature is or includes the *name* of the signatory. The proper view is that the signature permits the *identification* of the signatory, which is not the same thing.[4] There is a difference between asking "is this signed?" and "who signed it?"

Common law

Electronic signatures are arguably valid at common law. Canadian courts have tended not to make such general proclamations, but there are cases where they have simply proceeded to analyse the law applicable to them, essentially assuming their validity.

---

[1] John D. Gregory retired in 2016 as General Counsel, Ministry of the Attorney General (Ontario), where he developed legal policy on electronic commerce on the provincial, national and international levels. More material from John Gregory can be found at www.euclid.ca.

[2] Professor Chris Reed, "What is a Signature?" (2000) Journal of Information, Law & Technology https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/

[3] The current law of seals and the possibility of electronic seals are beyond the scope of this short article.

[4] The same is true for many areas of the law of electronic communications. For example, a requirement that information must be in writing says nothing about the durability of that writing. Durability needs to be a separate rule.

The most thorough analysis of the common law applicable to e-signatures has been done by the Law Commission of England and Wales. The Commission published an "Advice"[5] in 2000 that no law reform was needed to validate electronic signatures, and indeed law reform might raise doubts about the validity of signing methods not specifically mentioned.[6] The Law Commission revisited the question in 2018-19 and came to the same conclusion.[7]

Statute

Canadian jurisdictions have not relied on the common law to support electronic signatures; they have all passed legislation.[8]

Ontario's statute is the *Electronic Commerce Act, 2000*[9] ("*ECA*") — yes, over 20 years old. It says very simply that where the law requires a signature, that requirement is met by an electronic signature.[10] Because the common law is friendly to e-signatures, the statute did not go into much detail. The Act applies to e-signatures and e-documents whenever created, *i.e.*, before or after the Act came into force.[11]

An "electronic signature" means "information in electronic form that a person creates or adopts in order to sign a document and that is in, attached to or associated with a document".[12] Thus, the signature does not have to look like a handwritten signature, and it can be in a separate document if the link is clear.

The use of the verb "sign" is not circular or redundant: it is essential to the policy. The policy is that there is not a separate body of law for e-signatures. The mental and legal elements of an electronic signature are the same as those of any other signature.

The Canadian statutes are based on the UNICTRAL Model Law on Electronic Commerce[13] (1996). The Model Law, however, requires that the method used to identify the signatory should be "as reliable as appropriate in the circumstances". Canadian and particularly Ontario law does not impose a reliability requirement.[14]

---

[5] Law Commission of England and Wales, *Electronic Commerce: Formal Requirements in Commercial Transactions*, 2001, online: https://www.lawcom.gov.uk/project/electronic-commerce-formal-requirements-in-commercial-transactions/

[6] While that advice was reflected in subsequent English legislation, which provided for the admission of e-signatures in evidence, but which was silent on their validity, it did not seem to have had a strong impact on commercial practice.

[7] Law Commission, Electronic Signatures are Valid, confirms Law Commission (2019), online: https://www.lawcom.gov.uk/electronic-signatures-are-valid-confirms-law-commission/

[8] Canadian evidence statutes also generally permit reliance on electronic documents in legal proceedings as long as standard requirements about the document's authenticity and integrity are met.

[9] S.O. 2000, c. 17.

[10] *ECA*, s. 11.

[11] *ECA*, s. 25.1 (confirming what had been generally believed based on the language of the Act).

[12] *Electronic Commerce Act, 2000*, S.O. 2000, c. 17.

[13] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

[14] The Uniform Law Conference of Canada thought a reliability rule would be dangerous, in that it exposed the validity of the signature to judicial review, possibly years after the transaction in which the signature was used, and even if both parties were content with the method chosen at the time of the transaction and there was no doubt in practice about who signed what. See J.D. Gregory, "Must E-signatures be reliable?" (2013) Digital Evidence and Electronic Signature Law Review. https://journals.sas.ac.uk/deeslr/article/view/2024. Ontario's

As a general proposition, electronic documents do not have to be better — more reliable, more immune from alteration — than their paper equivalents. Many criticisms of e-documents could also be made of paper documents. People have learned to deal with the fallibility of paper. We will learn to do so for electronics too. The law should not invalidate them as we learn, or set up excessive barriers to their use.

Limitations

There are two legal limitations and one practical limitation to the statement that the *ECA* makes e-signatures valid.

The first legal limitation: the *ECA* says in effect 'where the law requires a signature', an e-signature will suffice. The law, however, rarely requires a signature; it does in wills, guarantees, some assignments and some land transfers, but not in most commercial transactions. This means that the parties can decide themselves whether to have a signature at all, rather than some other form of authentication, and if they want one, how to do it without regard to the Act.

The second legal limitation: the Act excludes a few kinds of documents (*e.g.* wills and codicils, trusts created by wills or codicils, powers of attorney with respect to individual financial affairs or personal care, and negotiable instruments). Thus, for those documents, one must look to other law, *e.g.* specialized statutes, to decide if they can be done electronically. Most still cannot.

The Act also says that it yields to any other law or regulation that authorizes or restricts the use of e-signatures.[15] It was not intended to prevent other government actions either before or after the Act came into force that specifically regulated e-signing. Thus, someone deciding whether and how to use e-signatures needs to be aware of other law that might apply. The exclusions are few.

The practical limitation: just because an e-signature may be legally effective does not make it prudent. The same is true of signatures on paper, of course. The *ECA* does not require reliability, but transacting parties, including governments, will almost always want the signature to be reliable, along with the rest of the documentation.[16] So the parties should consider their needs regarding execution, security, verifiability and the like. Depending on the

---

ECA authorizes a regulation imposing a reliability requirement for specific transactions or documents, but no such regulation has been made.

[15] *ECA*, s. 26. The main provincial enactments are found in some business statutes, though they sometimes refer to the ECA – and the ECA would almost certainly apply to them to the extent that they do not exclude or contradict it. The ECA also does not apply to federal laws. Much federal industry-specific legislation, including the *Bank Act*, *Insurance Companies Act* and *Trust and Loan Companies Act*, plus the *Income Tax Act (Canada)*, and their applicable regulations expressly recognize electronic signatures and sometimes spell out how to create such signatures for their purposes. (The federal statute dealing generally with electronic documents – *PIPEDA*, the *Personal Information Protection and Electronic Documents Act* – is of such narrow application as to be irrelevant to most business transactions.)

[16] Parties will always want reliable authentication, whether done by a signature or not. One may choose to rely on an unsigned document but not on a document whose source one does not know.

circumstances, the signature alone might not make the document or the authentication reliable; some other security feature might be appropriate.

The Act also says that nothing in it requires any person to use or accept information in electronic form without consent. (Such requirements may arise from other law.) The ability to say "No" to e-signatures or e-communications generally implies the right to say "Yes" if security or reliability are sufficient. Since the person who relies on a signature takes the risk that it is not genuine, parties will want to know what they should trust and insist on having it.[17]

Levels of security

There are many levels of security in e-signatures, just as there are for signatures on paper. For instance, paper documents may be initialled, signed simply, signed before a witness, signed before two witnesses both present at the same time (notably for wills), signed before a notary, and signed with a certificate of incumbency or authority to bind the party the signature represents.

Likewise, e-signatures offer a range of security, from a header of an email (held to be a signature by a Singapore court),[18] to a name typed at the bottom of an email, to a code exchanged privately between the parties, to a code that is part of a Public Key Infrastructure (PKI).

A simple example of an electronic signature without the use of software is where a person affixes a scanned version of their handwritten signature to an electronic document. This might be acceptable to the parties in low-risk situations, where the parties are known to each other, the transaction is of relatively low value or the chances of interception or misuse are negligeable.[19]

Risk assessments

What kind of e-signature will be acceptable to the parties, if any, depends on their threat-risk (TRA) assessments: what is the benefit of using e-communications, what are the risks (such as unauthorized alteration of documents after signing), what are the chances of the risks occurring, what harm can be caused by things going wrong compared to the cost of doing things more securely? Different parties will have different risk estimates and risk tolerance, and such differences will affect the use of e-signatures in transactions.

The COVID-19 pandemic has changed risk assessments, making the benefits of e-signatures greater, if not the other risks lower. And greater familiarity with e-communications generally helps lower the perceived risks

---

[17] The Act acknowledges that consent to using electronic communications may be implied from conduct (s. 5). Thus, buying from a website or responding to an email offer would indicate a willingness to do things electronically.

[18] *SM Integrated Transware Pte Ltd. V. Schenker Singapore (Pte) Ltd.*, [2005] 2 S.L.R. 651 (High Court).

[19] For an overview of the different types of remote signature available in Canada, how they work, and the risks, see Meyer Mechanic, "Understanding e-signatures" (LAWPRO, June 2, 2020) https://avoidaclaim.com/2020/understanding-e-signatures/. Not everybody would follow the statements in this piece in every particular, but it does indicate the kinds of thing one may choose to think about in the field.

E-signing software programs

The many commercial e-signing software programs now available also help lower the perceived risks. A number of businesses offer e-signing packages that keep track of who is who and what documents are signed in what order by what parties. They can assemble transaction books readily shared with all parties. They tend to solve some technical challenges, like being sure that a signature that one creates is used only for the document one intends to sign, and not transferred to some other document.

At least one of the commonly-used signing programs produces text in the document saying "E-signed by [name] on [date and time]." This formula can be a signature, but it is an awkward self-reference. It would be better if replaced by something purporting to be a signature, even simply a typed name followed by the words “electronically signed”, rather than just reporting on the fact of signature. It would be even better if the parties had expressly agreed to use the signing method that produces this formula.[20]

Conclusion

The law of e-signatures is not difficult. E-signatures will almost always be valid in law. The exceptions are limited and clearly defined. The practice of e-signatures, on the other hand, can be challenging. It may not be easy to agree about levels of security among all transacting parties and sometimes among the regulators of those transactions. However, increasingly standardized procedures and widespread use of recognized software enhance the profession’s and clients’ comfort with e-signatures. Not a moment too soon.

[20] Moreover, since the law does not usually require a signature, it might serve instead as a form of authentication, and there would be lots of machine-generated evidence to support it in that function.