Ensuring legal certainty in international electronic contracts

By John Wakefield and Cari-Dee Le

John Wakefield is a partner of Holman Webb Lawyers practising in dispute resolution.
Cari-Dee Le is an associate at Holman Webb Lawyers.

The Australian Government has been considering accession to the *2005 United Nations Convention on the Use of Electronic Communications in International Contracts* ('**Convention**'), which was adopted by the United Nations General Assembly on 23 November 2005 and entered into force on 1 March 2013. The purpose of the Convention is to facilitate the use of electronic communications in international trade by enhancing the legal effectiveness and commercial predictability of such communications in international contracts. It seeks to confer the same validity to and enforceability of paper based forms of communication and storage of information to contracts and communications that have been exchanged electronically. The Convention significantly facilitates trade by endorsing an enabling environment for paperless trade.

Some of the Convention's objectives are:

- to remove legal obstacles where electronic communications are used that may arise from the terms of international agreements concluded before the widespread use of electronic media;
- to foster the modernisation and harmonization of existing e-commerce legislation; and
- to provide jurisdictions that have not yet adopted laws on electronic transactions with a modern set of rules for both domestic and international application.

The first part of this article examines the international relevance of the Convention and provides a review of the previous regime in Australia, in particular the 1996 Model Law On Electronic Commerce ('**Model Law**'), followed by a discussion of the Convention's current status. The second part examines the main features of the domestic legislation focusing on some key amendments.

Snapshot

- Australia will soon be eligible to accede to the *2005 United Nations Convention on the Use of Electronic Communications in International Contracts*. The Convention also has current relevance as the Commonwealth, most states and territories (with the exception of Queensland) have made amendments to their respective electronic transactions legislation to reflect the new international standard (as per the Convention).
- The adoption of the Convention will remove any uncertainty with respect to the acceptability of the use of electronic communications in international contracting and enable parties to meet the written form requirements imposed by international treaties, such as the *Convention on the Recognition and Enforcement of Foreign Arbitral Awards* and the *United Nations Convention on Contracts for the International Sale of Goods*.

International relevance of the Convention

International relevance

For those countries that do not have laws on electronic commerce, the Convention provides a faster path to modernisation and uniformity. It offers legislators a set of internationally accepted rules to combat the challenges associated with amending domestic legislation. Many widely adopted international trade law treaties, such as the *Convention on the Recognition and Enforcement of Foreign Arbitral Awards* and the *United Nations Convention on Contracts for the International Sale of Goods* ('**CISG**'), of which Australia is a contracting party, contain certain formal requirements which obstruct the wide use of electronic communications. The adoption of the Convention removes any uncertainty with respect to the acceptability of the use of electronic communications to meet the written form requirements imposed by these treaties.

Current signatories

To date, 18 countries, including China, the Republic of Korea and Singapore, have signed the Convention. Several other States, including Australia, have started the consultation or implementation procedure to become a contracting party (see: www.uncitral.org/uncitral/en/uncitral_texts).

Previous regime & the Model Law

In Australia, the Commonwealth, states and territories have each developed their own electronic transaction legislation. All are largely based on the Model Law - a non-binding international instrument also developed by the United Nations Commission on International Trade Law ('**UNCITRAL**'), which sets out soft international norms relating to electronic contracts. The Model Law adopts a 'functional equivalent approach' to address the differences between electronic data and paper-based documents which is based on an analysis of the purposes and functions of paper-based documents. Electronic contracts become the effective equivalent of a paper based one.

The Convention updates and complements certain provisions in the Model Law in light of recent practice. It is UNCITRAL's first attempt to deal with electronic transactions in a binding international instrument and many concepts and rules relating to electronic records that originated from the Model Law have now become binding after ratification by Member States.

The legislative amendments aim to prevent dual international and domestic contract regimes. The fundamental rules with respect to the operative equivalents of writing, signatures, and originals in the Convention remain identical to those in the Model Law, however the Convention has a narrower scope. It applies to international contracts but not to contracts for personal, family or household purpose. Australia's *Electronic Transactions Acts* ('***ETA***'), continue to apply to business and consumer contracts alike.

Development in Australia

In 2007 the Standing Committee of Attorneys-General ('**SCAG**') agreed to consider updating Australia's model electronic transactions legislation to reflect the revisions to the Model Law contained in the Convention. In November 2008, the Commonwealth Attorney-General's Department released a consultation paper making 11 recommendations covering the necessary amendments to align Australia's laws with the new international standard, specifically the Convention. The states and territories consequently made legislative amendments to reflect the Convention. Queensland is the only state that has not amended its ETA. Once it does, Australia will be eligible to accede to the Convention.

In New South Wales, the *Electronic Transactions Act 2000* (NSW) ('***ETA* (NSW)**'), as amended by the *Electronic Transactions Amendment Act 2010* (NSW) ('***ETAA***'), regulates electronic transactions. The amending Act brings the current legislation in line with the international standards. The *Electronic Transactions Act 1999* (Cth) ('***ETA* (Cth)**') was also amended and applies for the purposes of a law of the Commonwealth.

Validity of electronic transactions

Under the *ETAs* a transaction will not be invalid because it took place wholly or partly by means of one or more electronic communications (*ETA* (Cth), s 8; *ETA* (NSW), s 7). Electronic communication is broadly defined to include emails, web-chat, phone-texting and voice recognition systems. This general rule is subject to other provisions of the legislation, which deal with the validity of transactions. Each state or territory also has regulations, which may exclude the application of the general rule to specified transactions and specified laws. Parties can agree to exclude or modify these default rules.

Writing

The *ETAs* provide that where a particular law permits or requires a person to give information in writing, that permission or requirement is deemed to be satisfied if the person provides the information via electronic communication (*ETA* (Cth), s 9; *ETA* (NSW), s 8). Generally, electronically communicated information is acceptable if it is reasonable to expect that the information will continue to be accessible in the future, and the recipient has given consent to receiving communication of the information electronically.

Signatures

In cases where parties are required by law to provide a signature, that requirement is satisfied if a method is used to identify the person and indicate his or her intention with respect to the communicated information (*ETA* (Cth), s 10; *ETA* (NSW), s 9). The method must also be as reliable as is appropriate for the purposes for which the information is communicated. The inclusion of this reliability test is to ensure the principle of functional equivalence is given the correct interpretation (see Explanatory Note to the Convention, para 163). Again, the recipient must consent to the use of this method.

Production of Documents

A party required or permitted by law to produce a document in hard copy may alternatively produce the document in electronic form (*ETA* (Cth), s 11; *ETA* (NSW), s 10). To be acceptable, the method of generating the electronic document must be reliable and the integrity of the information must be maintained. Again, it must be reasonable to expect that the information will be accessible in the future and the recipient must consent to the provision of an electronic document.

Consent

The *ETAs* contain a consent provision for electronic writing, signature and production provisions. The consent provision is absent from the Model Law on which the legislation was based. This provision is a serious weakness in the legislation as it conflicts with the principle of functional equivalence. From the Explanatory Memorandum to the *ETA* (Cth), the premise for a consent provision is that a person should not be compelled to use electronic communications. Essentially the consent provision requires parties to reach an agreement in advance as to the use of the particular electronic communication. Such consent may be reasonably inferred through conduct. The provision remains applicable even after amendments of the *ETA* to reflect the Convention.

Retention of information and documents

Under the *ETAs*, recording or retaining the information in electronic form may satisfy a requirement to record information in writing, to retain a document in hard copy or to retain information the subject of an electronic communication (*ETA* (Cth), s 12; *ETA* (NSW), s 11). To be acceptable, it must: (a) be reasonable to expect that the information will continue to be accessible in the future; and (b) the method of information storage must comply with the requirements of the regulations under the respective *ETAs*.

Where a document is required to be retained, the party must also retain information as to the origin and destination of the communication, and as to the time it was sent and received. The method for retaining the information must provide a reliable means to substantiate the integrity of the information.

Key amendments

Extended definitions

The amended legislation contains new and improved definitions. For example, the term 'place of business' has been expanded from the place of business of a government, government authority or non-profit body, to the place of business of an individual. The term 'transaction' now includes not only transactions of

a non-commercial nature but also:

(a) transactions in the nature of a contract, agreement or other arrangement; and
(b) any 'statement, declaration, demand, notice or request, including an offer and acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract, agreement or other arrangement' (*ETAA* (Cth), sch 1[2]; *ETAA* (NSW), sch1[6]).

Invitations to treat

Article 11 of the Convention has been incorporated in the domestic legislation (*ETA* (Cth), s 15B; *ETA* (NSW), s 14B). Unless otherwise clearly indicated, where a proposal to conclude a contract is made and communicated through electronic means to the general public and not addressed to specific parties, this will amount to an invitation to treat (that is, a request to others to make an offer or to engage in negotiations), rather than an offer whose acceptance would render a binding contract. This is in line with the corresponding provision of the CISG. In practice this means, for example that products displayed on a webpage will constitute an invitation to treat and not an offer. It is only when a customer elects to purchase a product and the item is placed in a virtual shopping cart that the personalised 'check-out' screen will constitute an offer.

Time of dispatch

Under the previous *ETA*, the time of dispatch of electronic communications was when the electronic message 'enters a single information system outside the control of the original'. This rule was problematic because with modern email systems the sender may retain the ability, and hence control, to recall sent emails, even from the recipient's inbox. The recent amendments to the *ETAs* modify the definition of 'time of dispatch', 'place of dispatch' and 'receipt of electronic communications' in line with article 10 of the Convention. The current definition speaks to previous concerns by clarifying that an electronic communication is taken to have been dispatched by the sender when it 'leaves an information system under the control' of the sender. Where it has not left an information system under the control of the sender, the time of dispatch will be when the addressee receives the electronic communication (*ETA* (Cth), s 13; *ETA* (NSW), s 12).

Time of receipt

The previous *ETA* defined the time of receipt as when the electronic message enters the designated information system of the recipient. However, it provided no definition for the designated information system. The designated information system could therefore be the personal computer of the recipient, or Internet Service Provider, or even where the recipient simply designates the internet. The amendment has simplified the test. An electronic communication is deemed as received by the addressee when it becomes 'capable of being retrieved' by the addressee at an electronic address designated by the addressee.

If the addressee has not designated an electronic address, the time of receipt will be: (a) when the electronic communication has become capable of being retrieved by the addressee; and (b) when the addressee has become aware that the electronic communication has been sent to that address (*ETA* (Cth), s 13A; *ETA* (NSW), s 12A). This is presumed to be when the electronic communication reaches the electronic address of the addressee (Explanatory Note to the Convention, at para 179). The amendments resolve the flaws of the former provision with respect to the designation on an information system.

Place of dispatch & receipt of electronic communications

These provisions have been updated. An electronic communication is taken to have been dispatched at the place where the originator has its place of business and to have been received at the place where the addressee has its place of business (*ETA* (Cth), s 13; *ETA* (NSW), s 12).

Automated message systems

The amended *ETAs* recognise a proliferation of automated message systems and confirms the enforceability of contracts entered into by such systems. Where computers enter into contracts automatically, the contract is not invalid, void or unenforceable on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract (*ETA* (Cth), s 15C; *ETA* (NSW), s 14C). The provision, however, seems to lack precision.

Input errors rectification

The amended *ETAs* now also consider circumstances where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and there is no opportunity to correct the error. In these cases, a party may withdraw the erroneous portion of the communication if they notify the other party of the error as soon as possible after becoming aware of it, provided no material benefit or value from any goods or services has been obtained (*ETA* (Cth), s 15D; *ETA* (NSW), s 14D).

Conclusion

The Electronic Communications Convention builds upon earlier instruments drafted by UNICTRAL, in particular, the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, which served as the inspiration for Australia's previous *Electronic Transactions Acts*. The main changes to the previous regime relate to: (a) extended definitions; (b) clarification of an invitation to treat in the electronic context; (c) amendments to the default rules for time and place of dispatch and receipt; (d) new rules to recognize the use of automated message systems; (e) Electronic signature and other form requirements; and (f) clarification of the location of parties rules.

Although Australia is not yet eligible to accede to the Convention, the *Electronic Transactions Acts* have been amended to accord with the Convention. These instruments have current significance. The case law on electronic communications is growing. However there is still relatively little guidance on the use of electronic signatures. While they go some way to address issues of uncertainty surrounding electronic communications in contracts in line with international norms, the full efficacy of these amendments remains to be seen. **LSJ**

Validity and enforceability of **electronic & digital signatures**

Troy Rollo is a barrister in Sydney and a member of the Law Society's Legal Technology Committee.

By Troy Rollo

Snapshot

- Two decisions last year have prompted doubts amongst practitioners about electronic signatures.
- Electronic signatures are not necessarily less reliable than ink on paper, but the risks do differ. With appropriate care, electronic signatures can be more reliable.

The September 2016 decision of the Court of Appeal in *Williams Group Australia Ltd v Crocker* [2016] NSWCA 265 prompted doubts electronic signatures are enforceable or binding. A decision in *In re Stanley Mayfield* (unreported, United States Bankruptcy Court, E.D. California, Bardwil J, 15 July 2016 (*'Mayfield'*), sanctioning a lawyer for submitting Court documents signed using DocuSign, without a paper document existing, raised similar concerns. While those doubts are unwarranted, practitioners need to account for the different (but not necessarily greater) risks of electronic signatures versus paper signatures.

Basic law of signatures

A signature is any mark applied to a document, intended, at that time, to be the signature of the signatory (*ex parte Myers* (1884) 10 VLR 322 at 324). Subject to any contrary statute, the mark could be a handwritten, typewritten or stamped name, a cross, or any other marking applied with that intention. The intention must be present when the mark is applied (*ex parte Gleeson* (1897) 22 VLR 485).

The mark can be made by the signer personally applying their mark, directing somebody (the amanuensis) in their presence to then and there apply a mark, or authorising somebody (the agent) to sign (*Thomson v McInnes* (1911) 112 CLR 562 at 573).

Where a statute requires a personal signature, the mark cannot be applied by an amanuensis or agent. This is a question of construction (*In re Whitley Partners Ltd* (1886) 32 Ch D 337) that does not require the words 'signed personally'.

Terminology

The term 'digital signature' is often, incorrectly, treated as interchangeable with 'electronic signature'.

An electronic signature is any mark applied to a document in electronic form, intended, at that time, to be the signature of the signatory. It is often a pasted in, scanned signature. The signature block at the bottom of emails can be a valid electronic signature (*The Corporation of the City of Adelaide v Corneloup* [2011] SASCFC 84 at [29]).

A digital signature (or 'cryptographic signature') is an electronic signature with a mathematical component, calculated using encryption technologies. Cryptographic signatures add a number to the document, derived from a secret number (the 'private key'). The private key has an associated, publicly disclosed, number (the 'public key'). The public key can be used to demonstrate mathematically, with very high confidence, that the cryptographic signature was applied by the person who knows the corresponding private key, and that the document is unaltered.

Relying on signatures

The main considerations in relying on signatures are:

- the degree of confidence, when receiving the document, that it was signed by the purported signatory; and
- assuming that person did sign, the provability if disavowed.

When receiving a paper document with a handwritten signature by a person whose signature is unknown to you, you may have no way of knowing it was signed by them, but if it was, proving it may be relatively easy – low confidence, better provability.

If you send a document to someone by email, and they send the document back with their signature pasted in, you might have more confidence it was signed by them (because the signer was able to receive the email), but there may be difficulty proving that if denied – low provability, better confidence.

The technologies used

In the decisions discussed, signatures were applied using the services 'DocuSign' and 'HelloFax'. There are other equivalent services. These services normally send an email to each intended signatory in turn, notifying the recipient to log into their account with the provider, or to click a link, to acknowledge and sign.

Depending on the service and the technology available to the signatory, the signer might type in their name, write it in on a mobile phone using their finger or a stylus, click 'I agree' to sign, or sign by another means. That is an electronic signature, not a cryptographic signature. This makes it harder to prove who signed the document. Even for signatures written with a stylus, the signature is easily duplicated, and physical depth of impression information embedded in a paper signature is unavailable.

These services typically add a cryptographic signature, using the service's private key, providing good evidence that the document was signed by the ordinary use of the service. Accordingly, proving that the disavowing signatory did sign may require proving the email was received by that person and no other, or that the person who logged into the account was that person and no other.

With this process the originally signed document, if one exists, is likely to be in the possession of the service provider, with only copies being sent to the parties. The service provider might even be making a copy of the document at each stage, without writing back to the original, so that there is no single document with all original signatures. Usually this is not a problem, because a copy is as good as the original.

The decisions

Williams Group v Crocker was discussed in a previous edition of the *Law Society Journal* (Paul Martin 'Electronic signatures: convenient but risky' 29, *The Law Society of NSW Journal*, December 2016, 81). Briefly, Crocker was a director of a company which used HelloFax to sign documents. Signatures, presumably scanned, were uploaded to HelloFax. One document, apparently signed by Crocker, was a director's personal guarantee of a loan given by Williams Group. Crocker had not changed his default password on HelloFax, and denied applying the signature. All Williams Group had was a fax, apparently signed next to Crocker's name.

The guarantee was in the form of a deed. Signing with these systems will ordinarily not satisfy the requirements for valid witnessing (see *Netglory v Caratti* [2013] WASC 364), preventing the document being a deed. Crocker did not apparently take this point.

Leaving that question aside, if the signature had been applied by Crocker, his amanuensis, or his authorised agent, and Williams Group could prove it, he would have been bound. However, Williams Group could not know, when receiving the faxed document, whose signature it was. Upon denial, there was no physical evidence demonstrating it was Crocker's. They had both low confidence and low provability.

The Court found the signature was not applied by Crocker. It was at law a forgery.

The decision in *Mayfield* involved signing of Court documents using DocuSign, and turned on a statutory requirement that the lawyer hold an 'originally signed document' (which cannot happen with DocuSign), and the Court's need for strong provability.

Enforceability of electronic signatures

There is no suggestion that an electronic signature is not binding. It is binding, if it otherwise meets the common law requirements. Both cases raise issues around the safety of relying on electronic signatures.

Electronic signatures are not necessarily less reliable than ink on paper, but the risks do differ. With appropriate care, electronic signatures can be more reliable.

Systems such as DocuSign and HelloSign can, when used appropriately, give some confidence that the document was signed by someone able to read email sent to a particular address. They add strong evidence from a third party that this is true. However, there remain risks:

- Email sent without encryption risks interception. Few practitioners are prepared to receive encrypted email;
- Many practitioners have their email printed by an assistant and read the printout. In that case, someone else always has first access;
- Many practitioners give their assistants access to their email;
- Solicitors commonly forward their email to someone else while away.

What do you need from the signature

Practitioners must understand what they need from the signature. Consider, in the context of the transaction:

- the level of confidence needed at transaction time;
- the means of proving the signature if disavowed (including, if a service is used, proving the operation and reliability of the service);
- whether the method is sufficiently reliable in the circumstances; and
- any statutory requirements peculiar to the type of document.

This requires understanding as to how the chosen process works and the security it provides.

Improving reliability – the retro approach

One way to improve reliability is to combine electronic signatures with ink on paper.

If the goal of electronic documents is faster completion after agreement, additional ink could be an early single page deed poll from the person sought to be bound, under which they agree to be bound by a signature later applied using the proposed mechanism.

If the goal is to keep the terms in electronic form or to minimise paper, additional ink could be a single page paper document agreeing to terms in an existing electronic document. The electronic document can be identified by a cryptographic hash – a number, generated from the contents of a document, in such a way that it is prohibitively difficult to generate another document with the same cryptographic hash. The terms are proved by showing that the cryptographic hash of the electronic document matches that on the paper.

One program that calculates cryptographic hashes is 'QuickHash'.

The high-tech approach

Cryptographic signatures improve reliability without paper. Practitioners wishing to familiarise themselves with cryptographic signatures can start by setting up their email software to send cryptographic signatures. The first step is to obtain a digital certificate. There are numerous providers of digital certificates for signing emails. Providers have instructions on the web, on setting up and using digital certificates.

Conclusion

The decisions discussed highlight the need for practitioners to understand how electronic signatures operate, what they need from the signature in a particular case, and how they can satisfy that need. **LSJ**