The write stuff? Recent developments in electronic signatures

*Paul Barnett, LL.M, Notary Public, Partner, Chapman Tripp Sheffield Young**

Paul Barnett is a Partner in the Wellington office of Chapman Tripp, solicitors. He heads the Technology Practice Group in that office. Paul has practised in the field of information technology since 1978. His team specialises in information technology and intellectual property.

PART 1. Introduction

In 1993 the New Yorker magazine published a cartoon of two dogs in front of a computer screen, with one saying to the other "On the internet nobody knows you're a dog."

Legal issues with respect to digital signatures are not easy to address since the digital world moves quickly and legislation and technology are constantly playing cat and mouse. Unquestionably, e-business will not meet its full potential unless there is a secure system(s) in place to confirm the accuracy and authenticity of electronic signatures.

Legislatures the world over have decided, or are deciding whether to regulate digital signatures and are seeking to ensure that an e-record or signature carries no less weight than a paper record or hand-written signature. The new laws do not make it compulsory for transactions to be conducted by electronic means or authenticated by e-signatures. Instead, they facilitate transactions that parties choose to conduct electronically.

Part 2 of this paper considers the recent legal development in relation to electronic and digital signatures in Australia and New Zealand. Emphasis will be placed on the need for the signature to be unique, so that only the user can create it and it is impossible to forge. Part 3 discusses the history of signatures and its legal function in society. Part 4 details how electronic signatures are made with an emphasis on a particular form of electronic signature called digital signatures. Part 5 discusses the advantages and disadvantages of using electronic signatures to do business.

PART 2. Legal developments in electronic and digital signatures in Australia and New Zealand

Signatures are the most commonly used form of identity verification in modern contract law, and are universally recognised as a symbol of a signer's intention to enter into legal relations. The development of electronic signatures allows us to enter into legal relations in electronic media, maximising the business opportunities provided by the internet.

Australia has passed laws implementing electronic signatures and New Zealand is preparing to do so. In 1999, the Australian Federal Parliament passed the *Electronic Transactions Act 1999* (ETA) and it came into force on 15 March 2000. The ETA covers only electronic communications with the Commonwealth Government and it is restricted to requirements under Commonwealth Statutes listed in regulations to the ETA.

Among the States and Territories, Victoria took the lead and passed the *Electronic Transactions (Victoria) Act 2000* which came into effect in September 2000 and more broadly encompasses "any law in force in [Victoria], whether written or unwritten" but does not include Commonwealth laws. The remaining States and Territories followed.[1] All these States and Territories laws are basically identical in their application. Queensland, however, does make one distinction in that the legislation does not apply to corporations law or corporations regulations.

The Australian State and Territory laws are also identical in that no-one will be forced to use electronic technologies. If they do, the electronic signature will only be effective if both parties consent to its use and if the method used was appropriately reliable.

The New Zealand Government's proposed Electronic Transactions Bill, which was tabled in the House of Representatives on 1 November 2000, will also give electronic forms of signatures the same legal status as hand-written signatures. The Bill has been delayed and is expected to be passed into law next year.

This is therefore, the dawn of a new era whereby electronic contracts and other digital documents can now have the same legal status as hard copy contracts, if properly signed.

Forward thinking institutions will be able to rely on digital signatures to enter into contracts and for other purposes, such as authorising regular payments.

For electronic signatures to be valid, it is pretty much a standard the world over that it must be authentic and accompanied by a valid reason for use. Software is being introduced to comply with these rules and as technology evolves, security concerns will be addressed accordingly.

PART 3. A history of signatures and their legal function

History of signatures

Signatures have existed since the development of print. The Sumerians, who are credited with the invention of writing, used seals to authenticate their writings, applied into their clay writing tablets using rollers.[2] The Talmud, which dates from the 3rd Century (Common Era), refers to signature and witnessing processes.[3] The Talmud also detailed security procedures to ensure documents were not changed after signing.

The use of hand-written signatures to authenticate documents began in the

Roman Empire at around AD 439, during the rule of Valentinian III. The *subscripto* was a small hand-written sentence at the end of a document, saying that the signer "subscribed" to the document. The Romans first used subscriptos to wills, but the practice spread to most other forms of legal transactions, and became a standard feature of Roman law, which itself is the basis of most Western common and civil law systems.[4]

In England signatures were first legally required in 1677, when the English Parliament passed "An Act for Prevention of Frauds and Perjuries".[5] The "Statute of Frauds" (as it became known) required "some note or memorandum in writing" that was "signed by the parties" for certain types of transactions. This requirement spread throughout most areas of English contract law, which the Australia and New Zealand legal system inherited virtually unchanged. Australia has since amended the Statute of Frauds in its jurisdictions. The relevant provisions[6] have been supplanted in the Australian Capital Territory[7]; New South Wales[8]; Queensland[9], and South Australia.[10] The relevant provisions still have force but are affected by local legislation in the Northern Territory, Tasmania, Victoria and Western Australia. New Zealand updated the law in 1956 with the Contracts Enforcement Act 1956.

Legal definitions and validity of "Signature"

There is no general statutory definition of "signature" in Australian and New Zealand statute law. Through many court cases over hundreds of years, judges have defined "signature" as containing these elements:

- Writing, drawing or affixing;[11]
- With your own hand;[12]
- A version of your own name, or your initials, or "any mark which identifies it as the act of the party"[13];
- With the intention of authenticating a document as being written by you, or legally binding on you.[14]

Rubber stamps with the name of a company or person are also legally valid to serve as a signature.[15] A person may also authorise another to sign documents on his or her behalf.[16] Long before the advent of electronic signatures, the law recognised the legal validity of facsimile signatures – an early victory for electronic commerce! [17]

PART 4. The need for electronic signatures

The importance of the internet as a new business marketplace cannot be over-estimated.

- By the end of the year 2003 it is estimated that 790 million people worldwide will be online.[18]
- By 2005 it is projected that one billion people, about 15% of the world's population, will be using the internet. Their use will fuel more than US$5 trillion in internet commerce, an increase of 70% from internet spending of US$354 billion in 2000.[19]
- More than 60% of Australians have internet access, with about half that amount having a home connection.[20]
- Just under 40% of New Zealanders currently have internet access at home.[21]

It would seem from these statistics that the future of business is with the internet and so it is crucial that identity in the form of digital signatures is accepted.

So, with a growing number of business deals operating online, how can documents in these deals be properly authenticated? How can parties to online agreements safely and efficiently identify themselves using electronic media forms?

Traditional, physical signatures have the benefit of being universally understood and used as well as being easy and cheap for people to use. They provide physical evidence that a person has seen and made connection with a particular document. The question is, can signatures be replicated or replaced satisfactorily in the electronic age?

What is an electronic signature?

A universally accepted technological standard does not exist. Definitions of "electronic signatures" tend to refer to the intentions of the parties to treat a signature as being legally binding. Because computer technology becomes obsolete so quickly, most definitions avoid specific descriptions of the form or content of an electronic signature.

For example, the Australian Electronic Commerce Expert Group (AECEG)[22] defined "electronic signature" as, "*Any symbol or method executed or adopted by a party with the present intention to be bound by or to authenticate a record, accomplished by electronic means*". The AECEG stated that this could include:

- typing your name at end of an electronic message;
- a fingerprint or retinal computer recognition; or
- an algorithm or other numerical sequence with unique document identifiers.

Software is currently being offered in the USA which analyses the shape of a physical signature and the dynamics as to how it was created, such as speed, pressure and timing. It also records hand movements through wind changes directly above the tablet when the stylus is not touching it. The success of this application has to be questioned in light of the fact that we seldom sign our name in exactly the same way twice. For example, how many times have you been asked to authorise credit card receipts for a second time because your first signature did not precisely match that on your card?

Biometrics, more commonly understood as face-identification software, could pave the way for a security system using a combination of face and voice recognition along with lip movement. Tests are currently being undertaken to enable users to create a profile by initiating the "record" mode, facing the camera, then repeating a word or phrase five times. This profile would replace the Windows Log-on screen when a PC is started up.

Alternatively, there is another product emerging that requires a user to press a fingertip on a small credit-card sized module to gain access to a PC. A user selects a finger to be used for indication, then presses the sensor three times to record information and four times to verify it. Data created from the fingertip is stored on the card.

It is important to emphasise that electronic signatures are *not* a graphical representation, scan or copy of your hand-written signature. Scans or copies of hand-written signatures, like most other graphics on the internet, can be forged or amended easily, and provide little protection to would-be signers.

Digital signatures[18] and encryption[23]

Digital signatures use encryption, a form of encoding which uses mathematical sequences called algorithms. To understand how these digital signatures work, it helps to know the basics of encryption.

Encryption is a popular option used for encoding documents by scrambling them into a jumbled numerical sequence. Encryption generates a "private information key" and a corresponding "public information key". These two keys are mathematically associated, but it is impossible to derive or encode one from the other. The private key is assigned to an individual signer, and known only to that person, but the public key can be freely circulated to others.

So, when you want to send a document, you encrypt it using your private signature key. No one else will be able to read or change the document except you (the private signature key holder) and a person with the matching public signature key.

How digital signatures work

As mentioned above, the signer generates or is provided with a private signature key and an associated public signature key. The signer generates a "message digest" of the document to be signed. This is the product of a hash function, which compresses a document of an indeterminately large size to a smaller, specifically-sized document. For example, a hash function can compress a 25,000-byte message to one of 16 bytes.

The signer provides the "message digest" and their private signature key as inputs to the signature algorithm. The output is a "signature value" (a jumbled sequence of letters and numbers) that gets appended to the bottom of the message. Here is a widely used example of a signature value:

----------BEGIN PGP SIGNATURE---------
Version: PGP for Personal Privacy 5.0
Charset: no conv

iQa/AwUBNDO/t7MyK9tbh/xKEQJBRwCg8O
TYnGYUXrNitSBxUNOU4sqsEkUAniIbYbjzf
PVU/LVUHJbU/eu6Xqqj
=dWr2

----------END PGP SIGNATURE----------

This jumbled sequence is unique to the document to which it has been attached. If someone else tries to sign the document, the numerical string will be different. If the signer or anyone else tries to change the document, even by one space bar or letter change, the string will also change.

Verifying digital signatures

For a signature to be regarded as valid, there needs to be proof of some kind of link between the signer and their electronic signature. This is easily achieved with hand-written signatures, which are physically linked to their signer (although still subject to forgery). Electronic signatures are also easily verified, using a "reverse" encryption process.

To verify an electronically signed message, a person needs the same hash function as used by the sender, and the signer's public signature key. The verification process works like this:

- The verifier inputs the hash function to generate another "message digest" over the received document. If the message has not been changed since it was signed, the two hash calculations should be the same.
- The verifier then obtains the signer's public signature key, and checks that it is authentic (see below).
- The verifier then inputs the message digest, the signature value and the public signature key into the signature algorithm. The algorithm will then indicate if the signature was valid when the message was first signed, and if it has been changed since signing.

Encryption processes using public and private signature keys require a trusted third party to check whether particular key signatures belong to specified persons. Just who that third party will be is one of the most challenging issues facing the development of electronic signatures.

Certification Agencies

Many jurisdictions using digital signatures have approved certification agencies which issue public key certificates to individual signers (binding the key to that signer's identity) and perform authenticating checks on signatures and signed documents. Certificates are usually issued for a limited period of time and may be renewed.

Certification agencies may be state-controlled (as in the Federal Republic of Germany), or privately-operated. Lawyers in the USA have also investigated setting up a "digital notary" network to authenticate documents, which works in a similar way to a public notary service. Further developments in this area are awaited.

Before issuing key signatures, certification agencies will require some evidence that you are who you say you are. Some agencies require key holders to give passport equivalent personal identification, whereas some agencies simply require a listing in a public phone directory. Most agencies will offer a range of verification services with differing degrees of security.

The success or failure of any digital signatures therefore depends on the reliability of a certification agency. A reliable agency must also be able to archive its files, so as to verify digital signatures when the signer's signature key has expired.

Public key infrastructure (PKI) has been identified as the key to universal secure electronic transactions. PKI

can be best described as the chain created by the certification agency signing the digital certificate with its own identification certificate to verify authenticity. This also promotes confidence and trust in the certificates issued. To this end PKI is being actively promoted.

An Australian company is exporting its PKI services to New Zealand. However, New Zealand is not able to export to Australia because the Federal Government has mandated that only Australian based companies can provide the crucial parts of the service including storage and maintenance of digital signatures for such services. New Zealand is still in the process of determining its certifying authority criteria but is likely to have more choices and options than Australia.

Overseas adoption of digital signatures[24]

Several overseas jurisdictions have passed legislation to implement digital signature processes. Examples are:

- the *Digital Signature Act 1995* (Utah);
- the *Digital Signature Act 1997* (Federal Republic of Germany);
- the *Electronic Communications Act 2000* (United Kingdom); and
- the *Electronic Signatures in Global and National Commerce Act 2000* (United States of America). Notably, President Clinton led the trend in signing the Act using both his hand-written and electronic signatures.

The Utah and German laws are technologically specific, regulating only encryption-style signature models. By comparison, the USA model regulates any electronically-recorded information which is adopted by a person with the intent to sign the agreement.[25] This non-technologically specific wording has a much wider coverage, regulating "I Agree" set-ups and digital thumbprint scans as well as encryption technologies.

Most e-signature laws establish State-regulated bodies for issuing key codes and licensing certification authorities, and allocate liability to those relying on signatures. In the Utah legislation, for example, recipients assume the risks of a forged signature if it is not reasonable to rely on the signature in the circumstances.

Part 5. The advantages and disadvantages of electronic signatures

Advantages of electronic signatures

Access to internet marketplaces

Electronic signatures allow parties to perform business transactions over the internet, and benefit from the speed, efficiency and wide market coverage the internet provides.

Less paper storage

Documents which can be finalised and signed online may be stored in an electronic format without the need for a paper original. This cuts down on the need for physical storage space, and decreases our reliance on paper, which can be lost, stolen or destroyed.

Better security

Because electronic signatures are unique identifiers, they provide almost guaranteed protection against forgery and changes to a document. Any changes and forgeries will be noted in the verification process, and all changes will be able to be documented. This provides much more security than simply stapling the pages of a paper document together.

Minimum Outside influence

There is less chance of human error, in that courier services can easily make costly mistakes, especially if the documents are time sensitive.

Better certainty of identity

Electronic signatures are much more efficient than existing forms of internet acceptances, which involve hitting "I Accept" buttons and entering credit card numbers. Online vendors have no foolproof way of proving you were the person who completed the transaction. So, in the inevitable case of third parties illegally making transactions with other peoples' names, online vendors frequently have to cancel the contract, thus losing revenue. Signatures give parties more certainty about the identity of a signer, as each public signature is connected to an individual. Therefore, it is less easy for a party to a digitally-signed online transaction to repudiate the action.

Disadvantages of electronic signatures

Problems with simplicity

Everyone understands hand-written signatures, and they are simple to verify. Digital signatures involve using a computer to perform a function on your behalf, and also require complex verification services. Because encryption is based on complex mathematical processes, users may have trouble understanding the processes involved.

Problems with control

When you write a signature, you perform a physical act (person to pen to page) under your direct control, which can be witnessed by other people. Digital signatures involve a computer, which performs a function on your behalf. If you stood up in court and said, "I didn't want to sign this document, but my pen made me do it!", no one would take you seriously. If you said "My computer made me do it," everyone understands how easily mistakes can occur or emails can be mistakenly sent on computers. For this reason, courts may be unwilling to enforce electronic signatures in contract disputes.

Problems with access

Hand-written signatures are practically universal and can be performed by both highly and marginally literate people. Computers, although becoming increasingly common, are still more expensive than pen and paper. Teaching a person how to use a computer is considerably more difficult than teaching a person how to sign their name.

Problems with verifying

Digital signatures require some kind of certification and verification regime. Should these functions be state controlled and regulated, or left to the private sector? There is also an ongoing problem about how to verify messages when private key codes have expired, or verification certificates lapse.

Problems with Deterioration

Unlike papyrus (the ancient Egyptians' choice of writing material) which can last for thousands of years, most computer hardware and software may only last for 5 or 10 years, and can be quickly rendered obsolete. certification agencies in the USA are now setting up archiving services, so it can be verified that particular certificates were valid at a particular time, and therefore that e-signed documents were validly signed.

Limitations on electronic signatures

Digital signatures are best suited for short-term contracts or documents which don't require extensive archiving, such as purchase orders, electronic funds transfers and contracts for access to online services.

Given the likelihood of rapid deterioration and technologies becoming obsolete, digital signatures probably will not be appropriate for birth certificates, wills, deeds or government records, unless sufficient archival facilities exist. They are also unlikely to be used for ceremonial occasions, like signing treaties.

Things to look for in digital signatures

If you are considering adopting electronic signatures for your business, you should consider the following points:

- Consider whether using electronic signatures will be appropriate for your business needs. If you are likely to require extensive archiving of documents, then digital signatures may not be your best option.
- Investigate local key certification services, and find out what level of security they provide.
- Ensure all employees using electronic signatures understand the processes involved. Given the "informal" nature of email, messages can be sent easily and almost immediately distributed, so it is important that employees using electronic signatures clearly intend to do so.
- Adopt a "company signature" protocol that automatically sends a signature and a disclaimer at the end of each message.

Part 6. Conclusions

Electronic signatures, if used prudently, can be an effective and secure way of doing business over the internet. Like all forms of identity verification, electronic signatures are not foolproof or immune to forgery. The success of electronic signatures is reliant on a legislative regime supportive of e-commerce, and a trustworthy certification agency.

As e-commerce continues to grow, it is likely that scepticism toward electronic signatures will disappear and they will become more commonly used and accepted. Review of the law, as progress is made, will undoubtedly initiate some changes based on feedback. However, given the popularity, accessibility and universal acceptance of hand-written signatures, it is unlikely that electronic signatures will fully overtake hand-written forms in the future.

---

* The author would like to acknowledge the assistance of John Forde, LL.B, B.A. (Hons.) in the preparation of this paper.

1 The Northern Territory ETA came into force in June 2001 and the Australian Capital Territory ETA came into force in March 2001. New South Wales, South Australia, Queensland and Tasmania have assented to their ETA's but they have yet to come into force.

2 Encyclopaedia Britannica, "Sumerian Language" and "Writing Systems", Brittannica.com Inc, 2000. Source: http://www.britannica.com/bcom/eb/article/9/0,5716,119409+6+110475,00.html. Fillingham, David, "A Comparison of Digital and Handwritten Signatures", *Ethics and Law on the Electronic Frontier,* Massachusetts Institute of Technology, Fall 1997.

3 Fillingham, *ibid*; Encyclopaedia Britannica, "Talmud" article,. Britannica.com, Inc, 2000. Source: http://www.britannica.com/bcom/eb/article/1/0,5716,72921+1+71073,00.html.

4 Fillingham, *ibid*; Nicholas, J. K., *An Introduction to Roman Law*, Clarenden Law Series, Oxford, 1962; Encyclopaedia Britannica, "Roman Law: The Law of Contract" Article, Britannica.com Inc, 2000. Source: http://www.britannica.com/bcom/eb/article/2/0,5716,115342+8+108633,00.html.

5 29 Car. 2, c.3.

6 see Statute of Frauds 1677, ss4 and 7.

7 see (ACT) Sale of Goods Act 1954, s3 (now repealed); (ACT) Imperial Acts (Substituted Provisions) Act 1986 s3(1), Sch 1.

8 see (NSW) Imperial Acts Application Act 1969 s8(1); (NSW) Sale of Goods (Amendment) Act 1988 s3, Sch 1 cl 2.

9 see (QLD) Statute of Frauds 1972 (repealed) s3 (repealed by the (QLD) Property law Act 1974)

10 see (SA) Statutes Amendment (Enforcement of Contracts) Act 1982, ss 3,4.

11 *Durrell* v *Evans* (1862) 1 H & C 174, 191, per Blackburn J; *Electronic Rentals Pty Ltd* v *Anderson* (1971) 124 CLR 27, 42 (High Court of Australia), per Windeyer J.

12 *Durrell* v *Evans*; *Electronic Rentals*; ibid.

13 *Morton* v *Copeland* (1855) 16 CB 517, 535, per Maule J.

14 *R* v *Kent Justices* L.R. 8 Q.B. 305.

15 *Goodman* v *Eban (J) Ltd* [1954] 1 All ER 763, 766, CA, per Evershed MR.

16 *London County Council* v *Agricultural Food Products Limited* [1955] 2 QB 218.

17 *Goodman* v *Eban*, ibid.

18 http://www.euromktg.com/globstats/.

19 PR Newswire 23/05/2001.

20 Sunday Telegraph (Australia) 24/06/2001 p37.

21 New Zealand Herald 03/07/2001.

22 *Electronic Commerce: Building the Legal Framework*, AECEG, 1998.

18 Any further references to "electronic signatures" will refer to all forms of electronic signatures, including digital (encryption) signatures and retinal or thumbprint scan

23 See: Fillingham, ibid; Moon, Peter, "Everything you always wanted to know about digital signatures", *Law Institute Journal*, December 1997.

24 *Electronic Commerce: Part One: a guide for the legal and business community*, New Zealand Law Commission, 1998, Chapter 7, "Electronic Signatures".

25 "Signing On the Electronic Line", *Computerworld New Zealand*, 25/9/00. Site: www.idg.net.nz/computerworld.