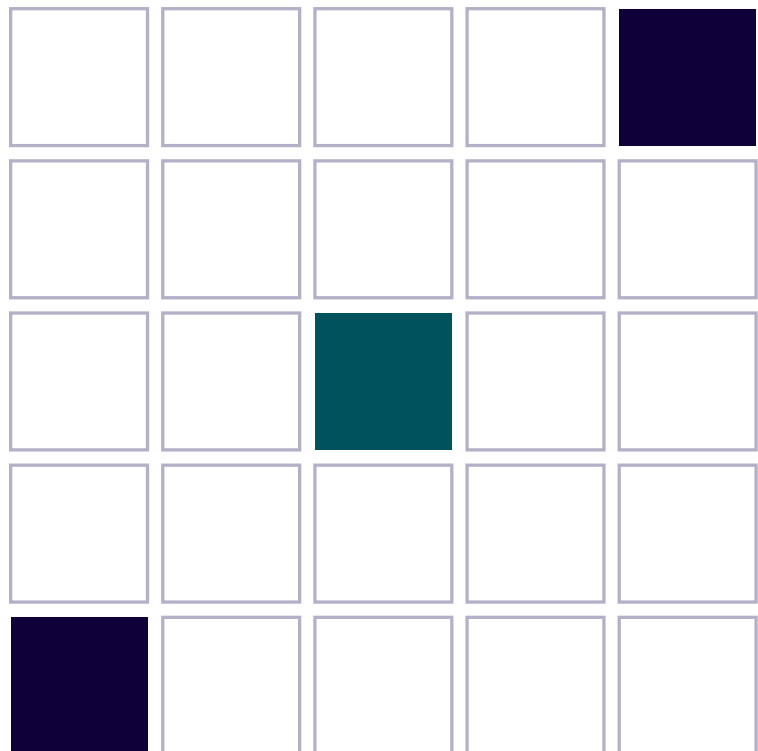


Electronic Transactions Act

Benefits for the Bold or Traps for the Unwary

Jeremy Salmond
Senior Associate
Bell Gully

Information Management Summit 2003



Bell Gully

Electronic Transaction Act

Benefits for Bold or Traps for the Unwary

Jeremy Salmond (Senior Associate)
Bell Gully, Wellington

Information Management Summit 2003

1. Introduction to the Electronic Transactions Act 2002

The purpose of the Electronic Transactions Act 2002 (ETA) is to facilitate the use of electronic technology by:

- (a) reducing uncertainty regarding:
 - (i) the legal effect of information that is in electronic form or that is communicated by electronic means; and
 - (ii) the time and place of dispatch and receipt of electronic communications; and
- (b) providing that certain paper-based legal requirements may be met by using electronic technology that is functionally equivalent to those legal requirements.¹

The extent to which the ETA achieves this purpose is still open for discussion but, in my view, having the ETA on the statute books is far better than having no ETA at all.

The ETA is one of the results of a lengthy consultation and policy development process in relation to laws affecting electronic commerce. This process commenced in 1998 with the issue of a Law Commission report on electronic commerce. This report was followed by further Law Commission reports in 1999 and 2000 and a Discussion Paper published by the Ministry of Economic Development in 2000.² Following the recommendations of the Law Commission, the ETA is closely based on the United Nations Commission on International Trade Law (**UNCITRAL**) Model Laws on Electronic Commerce³ and Electronic Signatures.⁴ The ETA also follows the approach of the Australian Electronic Transactions Act 1999.⁵

Despite being passed by Parliament late last year, **the ETA is not yet in full force** and will not come into full force until regulations clarifying the effect of the ETA on special legal requirements have been finalised (these special requirements include the effect on tax record requirements, credit contract notice requirements and notices about the destruction of dogs). That said, the ETA is expected to finally come into full force some time in November 2003.

Once the ETA comes into full force, it will be important to remember that the different parts of the ETA apply in different ways. At one level, the provisions clarifying the legal effect of electronic information and the default rules for electronic communications apply generally at law. On a more restricted level, the provisions of the ETA regarding satisfaction of legal requirements only apply to statutes and regulations.

So how will the ETA affect information management professionals?

¹ This purpose is described in section 3 of the ETA.

² Electronic Commerce : Part Three : Remaining Issues, Law Commission (NZ), 2000; Electronic Commerce : Part Two : A Basic Legal Framework, Law Commission, 1999; Electronic Commerce : Part One : A Guide For The Legal And Business Community, Law Commission, 1998; Discussion Paper: Electronic Transactions Bill, MED, May 2000; Links to these documents and other relevant resources are available at <http://www.med.govt.nz/irdev/elcom/transactions/index.html>

³ <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>

⁴ <http://www.uncitral.org/english/texts/electcom/ecommerceindex.htm>

⁵ <http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm>

If the ETA achieves its purpose of reducing uncertainty and permitting legal requirements to be met electronically then, based on the theory that business likes legal certainty, the ETA should stimulate growth in the processing of transactions electronically and storage of information in electronic formats (or at least remove a few of the impediments to such growth). This should stimulate business (and make life better?) for information management professionals. A better understanding of how (or if) this will occur can only be gained by working through the provisions and effect of the ETA.

2. Important Concepts

Before getting into the detail of the ETA, it is helpful to consider a couple of the important concepts that the ETA follows.

First, there is the concept of functional equivalence. That is, the ETA does not attempt to prescribe particular technologies as satisfactory equivalents to paper documents or written signatures but instead looks to the functions of paper documents and signatures and sets functional standards that must be met by electronic means. A helpful analogy is to think of music, the music effectively sounds the same whether it is stored on a CD or held in a computer as an MP3 file (although the technology and hardware used differs). In other words, it's the music that matters, not the media, hardware or technology.

The next important concept is technological neutrality. The ETA does not try and favour particular technology that could soon become outdated, or could become so standard (due to a legislative preference) that it stifles the development of better technology. Instead, the ETA uses very open language when referring to electronic communications and does not favour current encryption technologies, e.g. public key infrastructure. As a result, provided that a particular technology meets the broad functional requirements prescribed by the ETA, then that technology can be used to electronically manage information that is subject to paper based legal requirements covered by the ETA.

3. Validity of Electronic Information

The first substantive part of the ETA (section 8) states in plain terms that information is not denied legal effect because it is in electronic form or is in an electronic communication. The section goes on to clarify that information is not denied legal effect because it is referred to in an electronic communication intended to give rise to that legal effect (i.e., it is incorporated by reference into an electronic communication, for example by a hypertext link).

Although there may have been doubts in this regard when electronic commerce legislation was first contemplated (last century), there is no doubt that in 2003 this provision merely restates what the law is. That said, it is helpful to have this spelt out in black and white in our statute books.

What needs to be remembered though, is that if information is in an electronic communication then it is not "automatically" given legal effect. Electronic information is still subject to the same laws as any other information and can be rendered ineffective by those laws. For example, if an unusual or unexpected term is included in an offer, it should be clearly brought to the attention of the recipient and not "hidden" in the small print. This rule would apply whether the term is on a business's standard paper form or set out electronically in a website's access terms.

4. Default rules for Dispatch and Receipt

The second substantive part of the ETA (sections 9 to 13), sets out default rules that apply in respect of the time and place of dispatch and receipt of electronic communications. The time and place of a communication's dispatch and receipt can have important implications at law. By way of example:

- (a) if a notice has to be received within a certain period to be valid, clarity as to when the notice is received is necessary to be sure that the notice is valid; and
- (b) the place that a contract is formed is influenced by where an offer is received and this can affect the law that governs the contract and the service of legal proceedings in relation to that contract.

Despite the mobility that technology provides to business, these rules mean that certainty can be obtained as to where and when communications are considered to come from and be received

(that is, from a legal perspective). However, it is important to note that the rules set out by the ETA regarding dispatch and receipt are merely default rules. They can be easily overridden by agreement between the parties to the relevant communication. As a result, if your organisation has particular preferences in this regard, it should include relevant provisions in its standard terms. The ETA's default rules will also be overridden if particular legislation sets different rules for dispatch and receipt.

4.1 Time of Dispatch

Under section 10, an electronic communication is considered to be dispatched at the time it first enters an information system outside the control of the originator. By way of example, a text message will be deemed to be dispatched once the "OK" or "Send" button is pressed. However, an email from a PC on a corporate network would be deemed to be dispatched when the email passes out of that network, i.e., when it passes from the corporate mail server to the relevant ISP's server.

One question (that hopefully will remain theoretical) is when is an email deemed to be dispatched if it is sent internally through a corporate network to another PC on the same network (i.e., does it ever leave an information system that is outside the control of the originator). This could easily occur where consultants are seconded to a client or working on-site at a client's premises and receiving contractual or other sign-off from the client through the client's network.

4.2 Time of Receipt

Under section 11, an electronic communication is considered to be received at the time it enters an information system designated by the addressee for that purpose. If no information system has been designated then the communication is considered to be received at the time that it comes to the attention of the addressee. This raises a few questions about:

- (a) what is required to "designate" an information system; and
- (b) when does something come to your attention? When it arrives in your inbox, when you read the subject header, when you open it or when you read it?

It has been suggested that merely providing an email address on a letterhead will not amount to "designation"⁶, but there is a grey area between that and expressly requesting that responses be sent to a specific electronic address. To avoid doubt in this regard, one suggestion is to include wording in your standard email disclaimer clarifying that nothing in the email designates an information system for the purposes of section 11(a) of the New Zealand Electronic Transactions Act 2002, unless expressly stated otherwise. This ensures that emails are only deemed to be received when they come to your attention and the legal implications of important emails going to potentially unmonitored email addresses are mitigated.

4.3 Place of Dispatch

Section 12 states that electronic communications are considered to be dispatched from the originator's place of business or, if the originator does not have a place of business, from the originator's ordinary place of residence. If the originator has more than one place of business then the communication is considered to be dispatched from the place of business that has the closest relationship with the underlying transaction. If that test does not work then the communication is considered to come from the originator's principle place of business.

⁶ Electronic Transactions Act 2002: Plain Language Section by Section Explanation, Ministry of Economic Development, Information Technology Policy Group, Industry and Regional Development Branch, December 2002.

4.4 Place of Receipt

Section 13 states that electronic communications are considered to be received at the recipient's place of business or, if the originator does not have a place of business, at the recipient's ordinary place of residence. Similarly, if the recipient has more than one place of business then the communication is considered to be received at the place of business that has the closest relationship with the underlying transaction. If that test does not work then the communication is considered to be received at the recipient's principle place of business.

5. Satisfying Legal Requirements using Electronic Means

Part 3 of the ETA sets out how legal requirements in New Zealand statutes and regulations can be satisfied using electronic technology that is functionally equivalent to the paper-based measures contemplated by those legal requirements. When reference is made to legal requirements, this is reference solely to requirements in statutes or regulations. No changes are made to the common law. In brief, the legal requirements covered by the ETA are that:

- (a) information be in writing, or be given or recorded in writing;
- (b) information be written in a particular format or layout;
- (c) signatures be used;
- (d) signatures be witnessed;
- (e) documents or information be retained;
- (f) information be provided;
- (g) access to information be provided; and
- (h) originals be used.

Despite an extensive legislative audit during the development of the ETA, no one is entirely sure of the number of statutes and regulations that contain such requirements (i.e., that will be affected by the ETA). However, it seems that this is probably the part of the ETA that will be of most benefit to information management professionals, as it will enable a number of transactions that previously had to be paper-based to be conducted on-line or by email or other technologies. In other words, there should be a number of opportunities to introduce efficiencies into government and business operations through better information management systems and by increasing the use of electronic documents.

That said, there are a number of exclusions from the coverage of the ETA, the extent of which are considered in part 6 of this paper. In addition, this part of the ETA merely enables the use of electronic technology, *i.e., this part does not require anyone to use, provide or accept information in electronic form without their consent.*⁷

The breadth of the consent requirement in New Zealand can be contrasted with the Australian ETA, which provides that the consent of government agencies is not required, i.e., Australians can provide electronic information to government entities to meet legal requirements without first getting their consent. In Australia, this was seen as a lever that could be used to push government departments into the information age. It seems that such a lever was not considered necessary (or wanted) in New Zealand.

In relation to consent, it is important to consider what is meant by consent and the various methods of obtaining consent. Actual consent will obviously suffice in this regard, for example written or verbal consent. However, in addition, the ETA expressly states that consent can be inferred by conduct⁸. For example, sending information electronically could infer that the sender consents to receiving information electronically.

⁷ Section 16 of the ETA.

⁸ Section 16 of the ETA.

On a practical level, if you are looking to obtain the consent of customers then you should consider including an express provision in your terms of trade obtaining the necessary consent. Depending on the importance of the relevant requirements that will be met electronically, and standard practices in your industry, it may also be necessary to draw this consent provision to the attention of your customers. Where you have dealings with others (to meet legal requirements) then it may be a simple matter of forwarding them a letter asking for consent to meet those requirements electronically, and noting that if they don't respond but continue to deal with you then that conduct will be taken to indicate their consent.

5.1 Requirements for Writing

Under the ETA, if a legal requirement provides that information must be in writing, or be recorded or given in writing, then that requirement can be met electronically if the information is “readily accessible so as to be useable for a subsequent reference”⁹. This requirement is intended to be “functionally equivalent” to paper records. On a practical level, what is required to ensure that information is readily accessible so as to be useable for subsequent reference is not spelled out (as that would move away from the concept of technical neutrality).

In the first instance it will be up to information professionals (and their lawyers) to decide whether a particular information system meets the necessary standard.¹⁰ However, it is clear that the person responsible for recording or holding the information will need to maintain hardware, software and skills necessary to provide easy access to the information in the future. It may also be necessary to maintain back-up storage, to ensure that the information is readily accessible if the primary storage facility fails or is damaged. How long these responsibilities last will no doubt depend on the relevant legal requirement. On this basis, reverse compatibility and back-ups will be primary functional requirements for information management systems that are used to process information subject to legal requirements regarding writing. In addition, those implementing information management systems will no doubt seek assurances (and warranties) from their suppliers as to the future accessibility of the information on those systems.

Where information is to be given in writing, the recipient must consent to the information being given in electronic form or by means of an electronic communication. Where multiple copies of the same document are required to be given, this can be satisfied by giving a single electronic copy (given the ease of copying electronic information).¹¹ If a statute prescribes that a particular format or layout be used, or certain materials be used for writing, section 21 of the ETA clarifies that such requirements need not be complied with to meet a legal requirement using electronic means.

5.2 Requirements for Signatures

Before the days of computers and electronic communications, most people thought they knew what a signature was, i.e., a hand written scrawl of their name. However, the courts took a broader approach than this, and accepted simple marks by people who couldn't write, and even accepted marks from rubber stamps in some instances. The ETA takes a similar approach with “electronic signatures” and does not attempt to restrict what could be used, merely stating that in relation to information in electronic form, an electronic signature is “a method used to identify a person and indicate that person's approval of that information”¹². As a result, an electronic signature could comprise anything from an emoticon to a scanned copy of a hand written signature, through to a digital certificate certified by a trusted third party.

⁹ Sections 18, 19 and 20 of the ETA.

¹⁰ That is until a body of precedents builds up either through the courts or possible through industry practices and standards.

¹¹ Section 20.2 of the ETA.

¹² Section 5 of the ETA.

However, the ETA provides that for a legal requirement for a signature to be met by an electronic signature:

- (a) the electronic signature must adequately identify the signatory and adequately indicate the signatory's approval;
- (b) the electronic signature must be as reliable as appropriate given the purpose for which, and the circumstances in which, the signature is required; and
- (c) where the signed information is to be given to a person, the recipient has consented to receiving an electronic signature.¹³

Likewise if there is a legal requirement that a signature must be witnessed, then that requirement can be met by an electronic signature if the original signature is an electronic signature and the witness's signature meets the requirements outlined above (i.e., adequate identification, reliable as appropriate and the recipient consents).

What comprises "adequate identification" is an open question, and will remain so until principles are established through trial and error (and probably the courts), as the ETA gives no further guidance on this point. Looking at the level of identification that a paper signature gives, the threshold for electronic signature might not be set too high. However, it must be remembered that if you are using an electronic signature, you are one step removed from the actual signing (i.e., technology plays a much greater part). As a result, the threshold applied is likely to be higher than that applied to paper signatures.

Whether a particular electronic signature will be considered as reliable as appropriate is also an open question. However, on this point the ETA provides a presumption of reliability (albeit a rebuttable presumption) if:

- (a) the means of creating the electronic signature is linked to the signatory and to no other person (for example, an authorisation code known only to the signatory would suffice);
- (b) the means of creating the electronic signature is under the control of the signatory and of no other person; and
- (c) any alteration to the electronic signature made after the time of signing must be detectable.

In addition, if the signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing must be detectable. Providing assurance as to the integrity of information is a common function of a signature. This requirement ensures that in such cases there will be a presumption that the electronic signature is as reliable as appropriate only if the technology used to create the electronic signature would reveal any post-signing alteration to that information. Overall, this presumption seems to favour Public Key Infrastructure or biomechanical methods, contrary to the technology neutral aims of the ETA.

If the presumption cannot be relied on, guidance as to what is as reliable as appropriate will depend on practical, legal, technical and commercial factors. For example, very different requirements are likely to apply to a honey analysis certificate than the requirements that apply to a notice of strike affecting essential services.¹⁴ The Guide to the UNCITRAL Model law on Electronic Commerce (which is an aid to the interpretation of the ETA) also sets out a number of factors that should be considered in relation to reliability, including:

- (a) the sophistication of the equipment used by each of the parties;
- (b) the kind and size of the transaction;

¹³ Section 22 of the ETA.

¹⁴ Animal Products (Ancillary and Transitional Provisions) Act 1999 and the Employment Relations Act 2000

- (c) the function of signature requirements in a given statutory and regulatory environment;
- (d) the capability of communication systems;
- (e) the importance and the value of the information contained in the data message;
- (f) the availability of alternative methods of identification and the cost of implementation;
- (g) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and
- (h) any other relevant factor.

So if you are establishing an information management system that uses electronic signatures to meet legal requirements, you should consider whether the system you are establishing is “reliable as appropriate” in the circumstances, having regard to these factors. If possible, it is also sensible to get the recipient’s agreement to the type of signature to be used, as this will make it difficult for them to claim it was not sufficiently reliable at a later date.

That said, it is likely that the “safe harbour” provided by the rebuttable presumption of reliability will set a default standard for reliability. It may be very difficult to show appropriate reliability in other cases, especially if reliability is called into question before a court.

5.3 Requirements to Retain Information

Under section 25 of the ETA, a requirement to retain information that is originally in paper or some other non-electronic form can be met by retaining an electronic form of the information if:

- (a) the information is readily accessible so as to be useable for a subsequent reference; and
- (b) the electronic form provides a reliable means of assuring the maintenance of the integrity of the information.

The “readily accessible” requirement is considered above in paragraph 5.1. However, the additional requirement of maintaining integrity sets a high standard that is expanded upon in section 17. Section 17 states that the integrity of information is maintained only if the information has remained complete and unaltered, other than the addition of any endorsement, or any immaterial change, that arises in the normal course of communication, storage or display. The information system used to maintain the information must reliably prevent the alteration of the information. This seems to set a higher standard than that required for paper records.

In practice, following clear and well established guidelines for retention of electronic records should ensure that a reliable means of maintaining the integrity of the information is used (an example of such guidelines is the British Standards Institute document PD 0008:1999 - A code of practice for Legal Admissibility and Evidential Weight of Information Stored Electronically).

If the requirements of section 25 are met then, in most cases (i.e., subject to the exclusions from the ETA) electronic storage of records will be able to replace retention of hard copy records. However, in the public sector the policy objectives of the Archives Act are retained by the requirement that the Chief Archivist’s consent is required to the electronic retention of records subject to the Archives Act.¹⁵ It is anticipated that the Chief Archivist will issue general guidelines in this regard which presumably will set minimum standards, referring to particular technologies and reducing the technological neutrality of the ETA.

¹⁵ See the proviso in section 25(2) of the ETA.

In addition, Section 26 provides for the retention of information that is originally in electronic form, which may be retained:

- (a) electronically if it meets the “readily accessible” and “maintenance of integrity” tests; or
- (b) in paper form, if that will meet the “maintenance of integrity test”.

If the information being retained was in an electronic communication then, in addition to satisfying section 25, the following information (obtained by the person required to retain the information) must also be retained in a form that is readily accessible so as to be useable for a subsequent reference:

- (a) the origin of the electronic communication;
- (b) the destination of the electronic communication; and
- (c) the time of sending and receipt.

As a result, for information systems to comply with the requirements of the ETA, they should also include such information with electronic communications.

5.4 Requirements to Provide, Produce or Give Access to Information

Under section 28 of the ETA, a legal requirement to provide information, where that information is held in paper or another non-electronic form, can be met by providing information in electronic form if:

- (a) the form and means of the provision or production of the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, the information is required to be provided or produced;
- (b) the information is readily accessible so as to be usable for subsequent reference; and
- (c) the person to whom the information is required to be provided or produced consents to the information being provided or produced in an electronic form and, if applicable, by means of an electronic communication.

In addition, if the requirements of section 28 are satisfied, the electronic copy provided will meet requirements to provide an “original”.

Under section 29 of the ETA, information that is already in electronic form can be provided in its electronic form provided that the “maintenance of integrity” and “readily accessible” tests are met. Such information can also be provided in paper form, but if the maintenance of the integrity of the information cannot be assured then the recipient must be notified. The recipient is then able to require the provision of an electronic copy.

Again, the importance of maintaining the integrity of the information is important (i.e., keeping the information complete and unaltered), but in these sections this requirement is qualified by reference to the purposes the information is provided for, and the surrounding circumstances. As a result, it seems that the integrity of information to be provided electronically can be of a lower degree than the integrity of information retained electronically.

How the “readily accessible” requirement operates in these sections is not as clear. After the information is provided, who must ensure that the information that was provided is readily accessible and for how long? Must the person providing the information ensure it is readily accessible only at the time of provision, or also in the future? Given that information must be readily accessible “for subsequent reference”, it would seem that this imposes an ongoing obligation on the person providing the information.

That said, does the consent requirement mean that the recipient (and not the provider) must ensure it maintains reverse compatibility in its systems to enable future reference to the information? These questions become particularly important if encryption technology is used to “maintain the integrity” of the information. In this regard, who is responsible for ensuring that this technology, and the necessary keys, continue to be available? For example, if the information provided was encrypted and the recipient is provided with the key, does the provider need to ensure that the recipient can decrypt the information in the

future (and obtain replacement keys if the original is destroyed or corrupted)? Also, if third party encryption technology is used, must the provider ensure the recipient is permitted to use the relevant technology now and in the future?

Lastly, a requirement to provide access to information can be met electronically if the recipient consents and the form and means of access reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, the information is required to be provided or produced.¹⁶ If the access to electronic information is provided by providing the information on paper, and the maintenance of the integrity of the information cannot be assured, then the recipient of the access must be advised of this and provided with access to the information in electronic form, if requested.

6. Traps for the unwary

Although the ETA is intended to clarify the law, there are a number of traps that remain that reduce its effectiveness and, if not considered, could prove costly to those trying to rely on the ETA to move to greater electronic management of information.

6.1 The Exceptions

The first trap is that the provisions of part 3 of the ETA do not apply to all legal requirements. There is a long list of legal requirements, set out in the Schedule to the ETA, that cannot be met electronically. Some of the exceptions cover:

- (a) certain electoral and referenda legislation and regulations;
- (b) certain provisions in citizenship, civil aviation, door to door sales, credit repossession, fisheries, passport, criminal justice, penal institution, fisheries and a number of health related statutes and regulations;
- (c) notices that are required to be given to the public or attached to any thing or left or displayed in any place;
- (d) information that is required to be given in writing either in person or by registered post;
- (e) requirements to produce or serve a warrant or other document that authorises:
 - (i) entry on premises; or
 - (ii) the search of any person, place, or thing; or
 - (iii) the seizure of any thing;
- (f) wills and similar documents;
- (g) negotiable instruments;
- (h) bills of lading;
- (i) safety standards under the Fair Trading Act;
- (j) ship registration documents;
- (k) powers of attorney or enduring powers of attorney, affidavits, statutory declarations or other documents given on oath or affirmation; and
- (l) the practice or procedure of certain courts and tribunals, including the District Court, High Court and Court of Appeal.

In addition, if a particular kind of electronic information or technology is required by a specific legal requirement then that requirement is not overridden by the ETA.¹⁷ One example of this is the LandOnline system operated by Land Information New Zealand. The

¹⁶ Sections 30 and 31 of the ETA.

¹⁷ Section 14 of the ETA

legislation governing the operation of this system permits the Registrar-General of Land to specify particular technology that can be used to electronically file land transfer documents.

As a result, before relying boldly on the ETA to modernise any information management systems, you need to ensure that those modernisations are not going to be rendered useless by the exceptions to the ETA requiring the paper status quo to be retained or other specified technology to be used.

6.2 The Exceptions could be a Moving Target

The exceptions in the Schedule to the ETA can be changed by regulation, but those regulations must be confirmed by Parliament or they will expire between 6 and 18 months after the regulations come into force. In addition, the Schedule will be reviewed by the Ministry of Economic Development within 2 years of the ETA coming into force. Presumably the intent is to reduce the number of exceptions, but this is by no means certain. So make sure you've got the most recent version of the Schedule (or get good legal advice) if you are checking whether the exceptions affect you.

6.3 The Initial Regulations

Additional traps arise out of the proposed initial ETA regulations. Although these regulations have yet to be finalised, they are likely to set specific requirements for:

- (a) notices under the Credit Contracts Act - it is proposed that special rules apply regarding consent to the use of electronic notices and the time that an electronic notice is deemed to be received;
- (b) notices regarding the destruction of dogs under the National Parks Act and Conservation Act - it is proposed that special notice requirements apply; and
- (c) the retention of tax records - it is proposed that special conditions will apply to the electronic retention of paper-based records for the purposes of keeping records as required by the Tax Administration Act.

The special conditions will need to be complied with in information management systems implemented to take advantage of the ETA.

6.4 What does “Readily Accessible” Really Mean?

As mentioned above in paragraphs 5.1, 5.3 and 5.4, to satisfy legal requirements regarding writing or the retention or provision of information using electronic technology, the relevant information must be “readily accessible so as to be useable for subsequent reference”.

Just what is required to ensure that information is “readily accessible so as to be useable for subsequent reference” is not entirely clear. It may mean that systems developed in the future must be reverse compatible or that information must be in a generally acceptable or standard format. In any case, if you are trying to take advantage of the ETA by implementing a new information management system or otherwise, make sure the information stored in your system is readily accessible, and if you are relying on encryption (or compression) technology, make sure that you will have continued access to that technology in the future.

6.5 Compliant Systems Must Be “Reliable as Appropriate”

As mentioned above in paragraph 5.2, to satisfy legal requirements regarding signatures, an electronic system must be as reliable as appropriate given the purpose for which, and the circumstances in which, the signature is required.

You don't want to be caught with a system that is not considered to be “reliable as appropriate”. As a result, care will be required to ensure that your system is more than “reliable as appropriate”. What will be reliable as appropriate will need to be considered in the circumstances of the particular requirement and particular system. If the information technology industry establishes standards for what is appropriate in what circumstances, then those standards may influence how the ETA is applied.

7. Benefits for the Bold

7.1 Cost Savings

Compliance costs are often touted as a major hindrance to the operation of businesses, and they also affect the efficient running of government entities. The ETA offers the opportunity to lower those costs by using information management systems to electronically comply with a number of paper-based legal requirements. By way of example, instead of retaining bulky paper records off-site at significant expense, depending on the nature of those records, it may be possible to scan them and store them electronically. As a result, cost savings may be one of the main benefits of the ETA, provided its exceptions do not prove too expensive to cater for.

Consider where you have been required to use paper-based business to comply with legal requirements and think how you could move to more efficient electronic based systems. But remember that before you rush into implementing new systems, you need to ensure that those you are interacting with agree to the use of electronic information or systems, either through express agreement or changes to the “standard terms” that you have with those entities.

7.2 Opportunities for New Products

If you're in the business of supplying or developing information management products, ensure that those products can meet the requirements of the ETA. This will be an attractive selling point for those products. The suppliers of some products on the market have already recognised this and are promoting the ETA readiness of their products.

8. Getting Ready for the ETA

Whether or not you move to more efficient information management systems to take advantage of the ETA and electronically meet the legal requirements that your operations are currently subject to, you should think about doing the following to prepare for the ETA:

- (a) consider modifying your email disclaimer to clarify that just because you use email, you are not designating an information system under the ETA, i.e., state that nothing in the email designates an information system for the purposes of section 11(a) of the New Zealand Electronic Transactions Act 2002, unless expressly stated otherwise;
- (b) consider whether the default rules as to time and place of dispatch and receipt of electronic communications in the ETA are appropriate for your operations. If not, consider an alternative approach that is more appropriate and set out the alternative in your standard agreements and terms of trade;
- (c) check the “standard terms” of your suppliers carefully to ensure that you do not inadvertently agree to receiving information in electronic form (or electronic signatures) if your business processes cannot yet cope with this;
- (d) if you do plan to move to more efficient information management systems to electronically meet legal requirements, update your “terms of trade” to obtain the consent of your customers to these changes. However, to ensure that consent is gained it would be sensible to draw your customers’ attention to these changes too;
- (e) establish a policy about how your organisation will respond to requests that communications required to meet legal requirements be provided by others in electronic form. On a related note, consider which legal requirements covered by the ETA apply to your operations and how they might be met electronically by you or others. Even if you decide not to implement systems to take advantage of the ETA yourself, you will at least be aware of how others that you deal with might make changes to take advantage of the ETA; and
- (f) review your document retention practices to consider if cost savings can be made by moving to retention of electronic records instead.

9. Summary

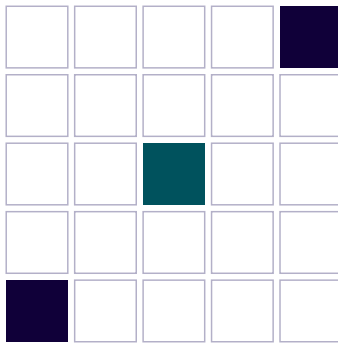
The ETA:

- (a) clarifies that information is not to be denied legal effect because it is in electronic form or in an electronic communication;
- (b) sets default rules for the place and time of despatch and receipt of electronic communications; and
- (c) clarifies that appropriate electronic information, methods and systems can be used to satisfy regulations and statutes that require that writing or signatures be used, signatures be witnessed or that information be retained or provided, and sets broad principles as to what electronic systems and methods might be considered appropriate.

However, the exceptions to the ETA and lack of clarity in key parts of the ETA mean that care is required if you want to rely on the ETA to replace existing paper-based systems with new information management systems and continue to comply with legal requirements. Despite the degree of care required, it is likely that the main benefit of the ETA will be the potential for cost savings in moving to more efficient information management systems.

Jeremy Salmond
Senior Associate
Bell Gully

Phone: 04 915 6951



Bell Gully

Auckland Wellington

Vero Centre, 48 Shortland Street HP Tower, 171 Featherston Street

PO Box 4199, Auckland, New Zealand, DX: CP20509 PO Box 1291, Wellington, New Zealand, DX: SX11164

Telephone 64 9 916 8800 Facsimile 64 9 916 8801 Telephone 64 4 473 7777 Facsimile 64 4 473 3845

www.bellgully.com