

**The Electronic Commerce Act, 2000 was introduced to ensure that consumers and businesses could engage in e-commerce easily and securely. Outline the main provisions of the act and critically analyse its objective.**

### Main Provisions

The Electronic commerce act has two simple functions:

- 1) To provide for the legal recognition of Electronic contracts
- 2) To implement the EU directive on electronic signatures

### Legal recognition of Electronic contracts

The electronic commerce act 2000 primary concerns itself with legally facilitating electronic transactions. The act was put in place to address the apparent deficiencies in existing legislation, which made frequent references to paper-based requirements and postage of documents. The act clearly specifies that electronic communications are now sufficient. The act defines an *electronic contact* as “A contract concluded wholly or partly by means of an electronic communication”.

But was this act completely necessary? Previous precedent states that the contract is concluded when the offeror receives the acceptance, however in cases where the communication is instantaneous then the postal rule does not apply and contracts are concluded as soon as notice of acceptance is received (*Entores Ltd Vs Miles Far East Corporation* [1955]). So this fits exactly into the architecture under which electronic commerce is carried out. In Part 2 of the act, clause 10 states that the electronic commerce act will not allow breach any other laws. In the UK, all legislation was painfully reviewed to ensure that it was applicable to electronic commerce; the Irish electronic commerce act was put in place to avoid this work.

One major and very serious flaw in the act is that the act indicates that a person may be bound by an e-mail that has not yet come to their attention. (For example: in cases where people do not regularly check their e-mail).

The Electronic commerce Act 2000 did not implement the European Union’s electronic commerce directive. This was only put into place in February 2003. These new Regulations provide for the free movement of Information Society services within the European Economic Area. These are essentially services (as distinct from products) provided 'on-line' between one Member State and another.

### Electronic Signatures

Electronic signatures are exactly what their name indicates, electronic identification and authentication; however, more specifically electronics must have the following 4 characteristics:

- 1) They must be uniquely linked to the signatory
- 2) They must be capable of identifying the signatory
- 3) They must be created using means that are capable of being maintained by the signatory under his or her sole control
- 4) They must be linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

So, an electronic signature is not something automatically applied to electronic communications (though obviously e-mail could be set up in this way). Also, they cannot be a simple signature image or piece of text. The electronic signature must

used to digitally sign the content of the communication. So, systems like PGP (Pretty Good Privacy) or any PKI (Public Key Infrastructure, e.g. Verisign) system that allows for the encoding and decoding of information, or even a simple MD5 Checksum of the content which verifies its content is technically required for a valid electronic signature.

However, access to these signing tools is quite limited. They can be sometimes expensive and using them can be difficult. While PGP can be integrated into Microsoft Outlook and other e-mail systems for organisations, no personal e-mail (GMail, Hotmail, Yahoo Mail, etc...) offers the facility to electronically sign e-mails. Further to that the certification service providers (e.g. Verisign) can be held liable for any damage done as a result of anyone relying on the signature if the provider has acted negligently. So, if I defraud the certification service provider and obtain hardware or software that allows me to electronically sign e-mails and documents as Bertie Ahern, Taoiseach of Ireland; then the certification service provider is liable for all damages caused by me with that signature.

But it gets worse. PKI can be easily broken (Breaking PKI, Dr Mike Scott). This was known pre-2000 and the example outlined is how to break PKI using Windows 98. So, while electronic signatures are a good idea and are now legally binding, their implementing architecture can be easily broken. (The Emperor's new Clothes, Jane Winn)

#### .ie domain names

For some bizarre reason, the electronic commerce act 2000 also puts into place strong laws regarding .ie domain names. In a move that would have been more at home in communist china, that law was enacted to not allow individuals to have a .ie domain name for personal use. So, I cannot buy <http://www.RonanCrowley.ie> but I can quite easily get <http://www.RonanCrowley.com> from an Irish company (for €9).

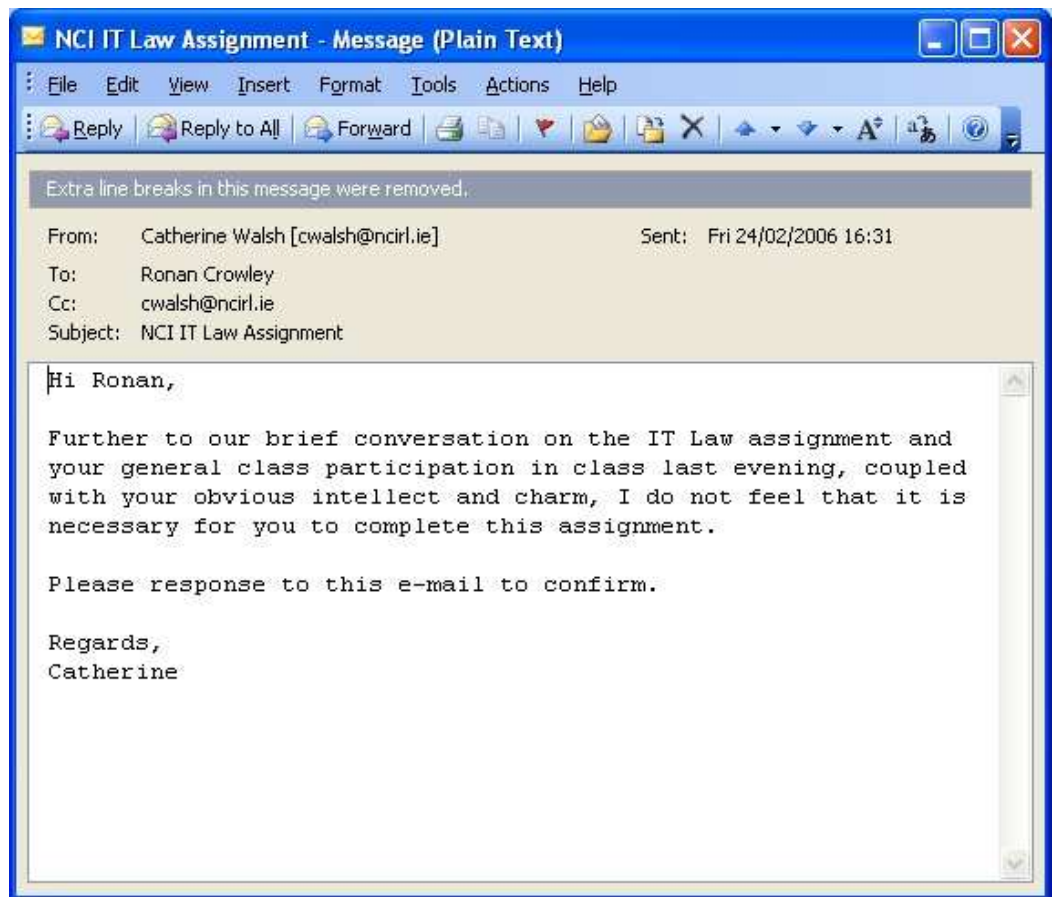
To register a .ie domain, you must be able to prove a real and substantive connection with Ireland. Usually this means providing a company registration number, or other documentary proof of your connection to Ireland, and rights to the name, which you wish to use. (IrishDomainNames.com). Why such a tight restriction? There is nothing to be gained from it, apart from the Irish government maintaining control over the Internet content delivered to the world from Ireland and the restriction of undesirable content, surely this is a restriction on the human right of freedom of speech?

#### A valid Electronic Contract?

Online fraud is a major blocking factor to electronic commerce. Many people that have not used the Internet for purchasing products or services cite fraud (specifically credit card fraud) as the most serious risk.

Electronic contracts, completed at time of receipt (i.e. Confirmation e-mail) do not require a response. So when you receive an e-mail, confirming the particulars of a contract organised previously in any manner, its safe to assume that the contract is correct and complete. But what if the e-mail is false? If a third party sends a falsified e-mail confirming the contract, unbeknownst to the recipient is this a valid contract?

I sent the mail below to myself (Its not difficult to fake an e-mail, using the "Mutt" e-mail program on any Unix environment, just press Alt+F to modify the *from* field before sending). It arrived seemingly from a valid e-mail address, and signed correctly. Regular e-mail usage would indicate that the mail is correct and valid.



However, the e-mail was a forgery and as such illegal and could not have resulted in a valid contract. But does this mean that there is a potential loophole in the electronic commerce act? I could set up an online shop selling mobile phones (for example), then in the very small print say that you are only buying a picture of the mobile phone, on the final purchase page, display the picture of the phone, legal contract complete. Then the customer gets a “confirmation” e-mail not sent by me, but rather someone else confirming that they will receive delivery soon. But they never receive the mobile phone.

The electronic commerce act makes no direct provisions for this scenario. There are no clear definitions of what terms and conditions are required to be displayed by law for transactions. Though admittedly, this would be almost impossible to enforce, as websites from all over the world can be used from Ireland.

#### Is the Act out of date already?

At the beginning of the act, under the definition of *electronic communication*, there is the stipulation that the definition “does not include information communicated in the form of speech unless the speech is processed at its destination by an automatic voice recognition system”.

Now this is a serious over-sight for two reasons. Firstly, voice recognition systems are notoriously difficult to implement, especially when adding any personal verification into the service, this I know from personal experience having written one (SVIS 2001). Secondly, and more importantly, the emergence of VOIP (Voice Over Internet Protocol) as a communications mechanism and direct substitution for the

existing PSTN (Public Switched Telephone Network, i.e. Current Eircom network) systems means that electronically communicated speech is a service that many people are currently using.

A huge amount of people are currently using Skype for their phone calls (Over 250 people have downloaded it) and more and more Irish people are replacing Eircom with the much cheaper VOIP solution offered by Blueface. So it is no longer appropriate to call VOIP a new or emerging technology. The fact that the electronic commerce act categorically states that this type of communication is outside the scope act, gives no legal standing to contracts conducted over the phone through VOIP connections. So this would indicate that phone calls carried out over VOIP connections are not legally binding in this state.

### Conclusion

The Electronic commerce act 2000 is a pretty shoddy piece of legislation. It seems to have been written without much technical knowledge or any foresight (Case and point VOIP). The necessity for the act in the first place was the need to categorically define electronic contracts. However, since the case of Entores Ltd Vs Miles Far East Corporation [1995], there was already an existing provision for this in the law. Secondly the EU directive on electronic signatures, but this has been proven to be based on a flawed technical system. So what has the electronic commerce act 2000 given us? A little bit of restriction over the .ie domain name, and not a lot else.

## References

Electronic Commerce Act, 2000

Course Notes

NCI, 2005

Catherine Walsh

“Sign of the times”

Article, Law Society Gazette

August/September 2000

PGP

Pretty Good Privacy

<http://www.pgp.com>

Breaking PKI

Dr Mike Scott, DCU

<http://www.computing.dcu.ie/~mike/pki.html>

The emperor’s new Clothes

Jane Winn

<http://civics.com/PKI/ShockingTruth.htm>

Irish Domain Names

Why register a .ie domain?

<http://www.irishdomains.com/WhyDotie.htm>

Domain Registry

<http://www.domainregistry.ie/RegistrationPolicy.php>

SVIS

Speaker Verification implemented Security

2001

<http://www.redbrick.dcu.ie/~bilco/project/>

Ronan Crowley & Paul Connolly

Mutt e-mail Client

<http://www.mutt.org>

Blueface

Irish VOIP Provider

<http://www.blueface.ie>

Skype

Worldwide VOIP provider

<http://www.skype.com>