THE SEARCH FOR ELUSIVE ELECTRONS: GETTING A SENSE FOR ELECTRONIC EVIDENCE

PAUL LAMBERT*

I. INTRODUCTION

> It is not an exaggeration to say that the most central problem in the whole of the law relating to computers, and perhaps more widely in the whole of contemporary law, is that concerned with adaptation of the legal process to deal efficiently with the introduction of modern technology.[1]

Never before has the pace of technological development moved so dramatically. Daily advances in communications and devices are expanding the range of business and personal activity. One should not assume that this is only relevant to a distinct section of society. Recent legislative advances also mean that contracts can now be completed electronically. It is inevitable that electronic evidence will increasingly be introduced before our courts.[2]

---

* B.A., LL.B., Commercial LL.M., CTMA, Solicitor, Information Technology Law Unit, Matheson Ormsby Prentice.

[1] Tapper, "Evanescent Evidence", (1993) 1(1) *International Journal of Law and Information Technology* 35. Note also Lambert, "Shareware: Problems of Definition and Legal Nature After the Oz Email Decision" (2000) 22 E.I.P.R. 595; Susskind, *Transforming the Law*.

[2] A case which may have used electronic evidence and in which a defendant pleaded guilty to maliciously publishing defamatory libels on the Internet is reported in "Man Gets Jail for Internet Libel of Teacher", the *Irish Times*, 21 September 1999. Emails were also used as evidence in the recent Microsoft antitrust case, see http://news.cnet.com/News/Pages/Special/Microsoft/msft_ruling.html, *USA v. Microsoft*, (US Appeals Court), 28 June 2001.

Some of the instruments for this change are the Electronic Signatures Directive,[3] the Electronic Commerce Directive,[4] the Irish Electronic Commerce Act[5] and similar legislative measures in other jurisdictions. While there have been cases in relation to electronic evidence prior to this these measures represent a clear recognition of the growth and emerging importance of both electronic and mobile commerce.

II. Electronic Evidence Heretofore

It was often considered that the hearsay and best evidence rules created difficulties for the introduction of electronic evidence. Others have argued that these rules are limited to written documents. In *Kajala v. Noble*[6] for example the court allowed a copy of a video tape to be introduced in evidence while the original remained with the BBC. The court in this instance was less concerned with the initial hurdle of admissibility than with the actual probity of the evidence. Another issue for electronic evidence was whether a printed letter was to be considered the original document or the actual file saved on computer. Vinelott J. considered this issue in *Derby v. Weldon (No. 9)* where he found in favour of the latter.[7] This decision could have consequences for the introduction of electronic originals.[8] There is also an important distinction between evidence generated automatically by a computer and electronic evidence generated by human intervention. The latter involves issues of

---

[3] Directive 1999/93/EC 13 December 1999 [1999] O.J. L013.

[4] Directive 2000/31/EC 8 June 2000 [2000] O.J. L178.

[5] The Electronic Commerce Act, 2000 does not fully implement the Directive. Work is currently under way to enact further legislation.

[6] [1982] 75 Cr. App. R. 149.

[7] [1991] 2 All E.R. 901. This case is commented upon by Tapper, "Evanescent Evidence", (1993) 1 *International Journal of Law and Information Technology* 35, 42.

[8] See "Electronic Originals" section below.

hearsay.[9] The case of *Myers v. DPP*[10] is one authority for this proposition i.e. that an electronic record based upon data inputted by a person amounts to hearsay. This case involved the identity of a vehicle using engine numbers. Distinguishing between these two categories is not always an easy task.

There are also other difficulties. For instance, following the Stephen Lawrence enquiry in the UK, a number of racist letters appeared in the email system of the Ealing Metropolitan Police Service (MPS). The subsequent investigation concentrated on computer evidence. Eventually PS Verdi (a police officer) was charged in relation to the emails. The MPS relied upon expert computer evidence which used a variety of (new) techniques.[11] These techniques sought to:

1. re-construct the original documents;

2. match print runs in event logs against reconstructed documents; and

3. identify the logged on User IDs responsible for the identified print runs.

Partly as a result of this expert evidence Verdi was dismissed. He in turn brought an employment claim for racism. Two computer experts testified for each party at the hearing. It was shown that some of the letters appeared to have been created days before being printed at the police station. This conflicted with earlier suggestions made by the MPS experts in relation to when the documents were produced. The tribunal found (a) that there was no evidence that the emails had been produced during the print runs previously identified by the MPS experts and (b) that there was no evidence linking Verdi to the emails in question.

---

[9] Tapper, (1993) 1 *International Journal of Law and Information Technology* 35, 52.

[10] [1965] A.C. 1001.

[11] See generally Turner, "Beware: Computer Evidence Quicksand" March 2001 *Computers and Law* 36.

Subsequently an apology and offer of reinstatement were made. Verdi was also awarded £150,000 compensation.

This case is also interesting because it highlights the standard procedures (in criminal investigations) for making an exact image of the (original) computer memory i.e. "imaging". This exact copy can be taken away, examined and relied upon in evidence. The procedures were not followed in this instance. The MPS experts used their own document reconstruction procedures. Anomalies and contamination were argued to have occurred. Evidence given on behalf of Verdi indicated that the failure to secure an "image" of the relevant computer servers "in a timely fashion" had irretrievably lost or contaminated any relevant evidence. In addition the MPS Principles of Computer Based Evidence also appear to have been ignored.[12] It is unclear what procedures would be followed in Ireland in civil and criminal cases.

It is arguable, for example, that there should be a chain of evidence listing all of those who held or were responsible for the image up until it was actually examined and extracts produced. There is also an argument for making a number of images, one of which is provided to the defence/respondent. This already occurs in relation to evidence (e.g. blood samples) in certain types of traffic cases.

Issues of definition also arise in relation to electronic evidence. In the case of *R v. Brown*[13] a police officer accessed information on the Police National Computer for a debt collection agency. The issue revolved around whether temporary access (i.e. viewing the information on the computer screen) was "use" in contravention of data protection law. The House of Lords (surprisingly) held that such access was not "use" for the purposes of UK data protection law. Lord Griffiths dissented. This arguably differs from what many had previously understood to be the position.

[12] Turner, March 2001 *Computers and Law* 36, 37.

[13] [1996] 1 All E.R. 545, cited in Hoey, "Techno-Cops: Information Technology and Law Enforcement", (1998) 6(1) *International Journal of Law and Information Technology* 69, 79.

The Criminal Damage Act 1991 and the UK equivalent (the Computer Misuse Act 1990) also create offences which involve wide definitions of "misuse" in relation to computers. While this article does not address the issues in criminal cases it can be said that criminal convictions in relation to alleged breaches of the UK Act have frequently proved difficult.[14] This may also prove to be the case in Ireland.

Technology is used more frequently in law enforcement and the wider legal process generally. Law enforcement agencies use technology to streamline normal tasks and procedures. They also use IT for investigations; surveillance; intelligence gathering; profiling; command and control, etc.[15] CCTV is also popular with law enforcement agencies, security firms, businesses and individuals themselves.[16] Computer animation and simulations are also being used more frequently although over reliance has been cautioned against.[17] Overall this means that electronic evidence will increase in its frequency before the courts. In addition recent legislative measures seek to make it easier to introduce electronic evidence.

III. Legislative Measures

A. Uncitral

One of the main pre-cursors to recent regulatory measures providing for electronic contracts was the United Nations Commission on International Trade (otherwise known

---

[14] *DPP v. Bignell*, *The Times*, 6 June 1997.

[15] See generally Hoey, (1998) 6(1) *International Journal of Law and Information Technology* 69.

[16] See generally Fay, "Tough on Crime, Tough on Civil Liberties: Some Negative Aspects of British Wholesale Adoption of CCTV Surveillance During the 1990s", (1998) 12 (2) *International Review of Law,Computers and Technology* 315.

[17] Nicoll, "Should Computers be Trusted? Hearsay and Authentication with Special Reference to Electronic Commerce", (1999) *Journal of Business Law* 332, 356.

as UNCITRAL). UNCITRAL established a working group which eventually culminated in the adoption of the UNCITRAL Model Law on Electronic Commerce in 1996 (the "UNCITRAL Model Law"). It was considered necessary by UNCITRAL to provide for equivalence between paper and electronic documentation. While the UNCITRAL Model Law has been described by one commentator as "timid" it has heightened the level of interest internationally on the issue of computer evidence.[18]

B. Rationale For Electronic Commerce Directive

The Electronic Commerce Directive is just one of the measures prioritised by the EU to assist the developing knowledge based economy and Information Society.[19] The EU Commission points out that the global electronic commerce market could be worth US$1.4 trillion by 2003. Already European electronic commerce is worth €71 billion and is expected to reach €340 billion by 2002.[20] Electronic commerce will fundamentally affect all aspects of human activity. Already e-government or electronic government is beginning to take off in Ireland. The Revenue Commissioners for example facilitate the filing of electronic tax returns.[21]

One of the main reasons behind these legislative endeavours is the necessity to ensure consumer confidence in electronic communications and transactions. Recitals 5, 38 and 40 (for example) of the Electronic Commerce Directive refer to existing "legal obstacles" and "divergences in legislation" which lead to legal uncertainty regarding

---

[18] Nicoll, (1999) *Journal of Business Law* 332.

[19] This was one of the results of the Lisbon Summit, see "Electronic Commerce: Commission Welcomes Final Adoption of Legal Framework Directive", at http://www.europa.eu.int/conn/internal/_market/en/media/eleccomn/ 2K-442.htm, accessed on 20 July, 2000.

[20] http://www.europa.eu.int/conn/internal/_market/en/media/ eleccomn/ 2K-442.htm.

[21] See Kelleher, "Electronic Government" (2001) 2 *Technology & Entertainment Law Journal* 13.

electronic commerce. Recital 7 also refers to legal certainty and "consumer confidence" issues. The objective of the Directive is to create a legal framework to ensure the free movement of Information Society Services between Member States.[22] Information Society Services are services normally provided for remuneration at a distance by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service (Recital 17).

The Directive provides generally that each Member State will amend its legislation appropriately to make contracts concluded electronically workable.[23] Article 1(2) sets out that the aim of the Directive is, *inter alia*, to approximate the law of the internal market in relation to electronic communications and contracts. Article 11 outlines certain provisions in relation to the placing of orders. When the recipient of services places an order through technological means the following criteria apply:

1. The service provider must acknowledge receipt of the recipients order without "undue delay and by electronic means," and

2. The order and acknowledgement of receipt are deemed received when the addressee is able to access them.

C. Electronic Commerce Act, 2000

The Electronic Commerce Act is clearly relevant to any discussion on electronic evidence. It immediately establishes that it encompasses "electronic contracts, electronic writing, electronic signatures and original information in electronic form in relation to commercial and non-commercial transactions and dealings and other matters,

---

[22] See Recital 8 of the Electronic Commerce Directive.

[23] See Recital 34 of the Electronic Commerce Directive.

[including] the admissibility of evidence in relation to such matters…"[24]

While previously there may have been some doubt as to the evidential value of electronic evidence, the Electronic Commerce Act (which came into force on 20 September 2000[25]) puts the validity of such evidence beyond doubt. The validity of electronic records cannot be denied solely upon the basis that they are in electronic form. Of course such evidence will have to be considered in the factual circumstances. While something may be admissible in evidence, that does not necessarily mean that such evidence will be relied upon by a court. Generally evidence must satisfy primary thresholds of admissibility e.g. the best evidence, exclusionary and relevancy rules. The Electronic Commerce Act does not do away with these rules. It merely makes it easier for electronic evidence to overcome the primary thresholds.

Part II of the Act provides for legal recognition and non-discrimination in respect of electronic signatures, originals, contracts and related matters. Section 9 indicates that information, including information incorporated by reference shall not be denied legal effect, validity or enforceability solely on the ground that it is wholly/partly in electronic form, whether as an electronic communication, or otherwise. It may take a number of fully contested cases before we can establish the exact boundaries of what electronic evidence will be both admissible and more importantly relied upon.

Section 22 of the Electronic Commerce Act provides that:

> In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility in evidence of … an electronic communication, an electronic

---

[24] Preamble to Electronic Commerce Act.

[25] Electronic Commerce Act, 2000 (Commencement) Order, 2000, S.I. No. 293 of 2000.

> … document, an electronic contract, or writing in electronic form … on the sole ground that it is [in] electronic [form] … or … if it is the best evidence that the person or public body adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

There were no major Irish legal cases in relation to electronic evidence. The Electronic Commerce Act now overcomes any lingering doubts which may have existed. It should be borne in mind however that the Electronic Commerce Act does not apply to the excluded areas such as laws dealing with wills, trusts, Powers of Attorney or dealings in property.[26] The Electronic Commerce Act also has separate provisions in relation to electronic writing, electronic signatures and other matters which are described below.

D. Electronic Writing

As a result of the Electronic Commerce Act, if a law requires or permits the giving of information in writing it will now be possible to give that information in electronic form, whether as an electronic communication or otherwise.[27] There is a qualification to this however. This may only occur:

1. if at the time the information is given it is reasonable to expect that it is readily accessible to the person or public body to whom it is directed;
2. if the public body consents and if the public body requires particular requirements that these requirements have been met;

---

[26] The excluded laws are set out in Section 10 of the Act. The Act does not affect (a) laws relating to wills and testamentary instruments; trusts or enduring powers of attorney; (b) laws in relation to property; (c) laws governing affidavits or declarations; or (d) rules and procedures of courts or tribunals. Section 11 of the Act also makes certain other exclusions, for example in relation to the Criminal Evidence Act, 1992.

[27] Section 12. This is inspired by Article 6 of the UNCITRAL Model Law.

3. if a person who is not a public body consents to the information being given in that form.

This is without prejudice to any other law requiring/permitting information to be given in accordance with particular information technology and procedural requirements or on a particular kind of data storage device or by means of a particular kind of electronic communication.[28] The giving of information includes but is not limited to making an application, claim, return, request, unsworn declaration, certificate etc.[29]

E. Electronic Signatures

If a law requires that a signature is required or permitted an electronic signature may be used.[30] However, an electronic signature may only be used:

1. if for a public body, the public body consents and any requirements have been met; and
2. if not for a public body, that person consents to the use of the electronic signature.

Various concerns have existed in relation to electronic commerce transactions. These include *authenticity* (i.e. that the message comes from the person it is said to come from), *integrity* (i.e. the content of the message has not been altered during transmission) and *non-repudiation* (i.e. that the sender cannot deny that they have sent the message e.g. they cannot deny entering into the contract). Electronic signatures attempt to solve these problems. An electronic signature should really be understood as an "electronic symbol" which helps to achieve the same aims which a wet paper signature is expected to achieve.[31] The most widely used method of

---

[28] Section 12(3).

[29] Section 12(5).

[30] Section 15. The origin is Article 7 of the UNCITRAL Model Law.

[31] Baker, "Security and Encryption", paper given at conference on *Legal Aspects of International E-Commerce* in Dublin, 10-11 May 2001,

verification is public key cryptography (PKI). This relies upon a public key and a private key. The sender's private key encrypts a message. Only the public key which is available to the recipient can decrypt the message. Thus messages can be sent safely and the person receiving it is assured that it has not been altered in transmission.[32]

Baker, an international expert in the field of security law, raises a number of questions about the enforceability of electronic agreements:

1. Does law permit parties to agree on what constitutes a signature? Will that agreement be given effect?
2. Does law permit parties to apportion liability by agreement (e.g. for compromise or disclosure of the private key)?
3. Will the agreement be given effect in all necessary jurisdictions?

While the Electronic Commerce Act is welcome, it does not fully implement the Electronic Commerce Directive. Even after full implementation some of the issues posed by Baker will remain. While the parties may agree to the use of electronic or digital signatures will this matter if they reside in a jurisdiction which has not enacted electronic commerce legislation? What happens if the parties agree to use electronic or digital signatures but their respective jurisdictions provides different measures in relation to the receipt and acknowledgment of communications or in relation to electronic contract formation?

The UNCITRAL Model Law has been the impetus of debate but Baker feels that many of its provisions are less than desirable and are in fact counterproductive. In addition, while the US approach is more favourable he feels the EU approach is being adopted by more jurisdictions internationally. He

organised by Hawksmere.

[32] Section 7 of the UK Act provides that electronic signatures shall be admissible in legal proceedings as to authenticity and integrity of communications.

feels that it is best not to rely on law alone to solve these problems but rather to cater for them by contractual agreement.[33]

F. Advanced Electronic Signatures

Section 14(2) of the Electronic Commerce Act states that an advanced electronic signature based on a "qualified certificate" may only be used:

1. if the signature required/permitted to be witnessed is part of a document to be given to a public body and the public body consents and if the body requires compliance with particular requirements that these requirements have been met; and
2. if not a public body the person consents to the use of an advanced electronic signature based on a qualified certificate.

G. Signatures Requiring Witnesses

If a law requires a signature on a document to be witnessed that requirement is met if:

1. the signature to be witnessed is an advanced electronic signature based on a qualified certificate of the person/public body by whom the document is required to be signed;
2. the document contains an indication that the signature of that person/public body is required to be witnessed; and
3. the signature of the person purporting to witness the signature is an advanced electronic signature based upon a qualified certificate.[34]

H. Defamation

---

[33] Baker, "Security and Encryption", paper given at conference on *Legal Aspects of International E-Commerce* in Dublin, 10-11 May 2001, organised by Hawksmere.

[34] Section 14.

Section 23 of the Electronic Commerce Act provides that defamation law shall apply to all electronic communications in Ireland including the retention of information electronically. Cases already establish that Internet communications can constitute a publication for the purposes of defamation law.[35] Plaintiffs have also sued internet service providers (ISPs)[36] for the defamatory statements of third parties. This is because it may often be difficult to establish the identity of the individual in question coupled with the fact that the ISP may often have the "deepest pockets."[37] ISPs argue that they are a mere conduit and have no knowledge of or part in the creation of the communication itself. They merely assist in transferring the message from A to B.[38] US cases against ISPs may diminish in frequency following the enactment of the Communications Decency Act, 1996.[39] Section 230 of this Act states that:

> No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information or any information provided by another information content provider.

This may also occur in the EU as the Electronic Commerce Directive provides a number of intermediary or mere conduit defences. In the case of *Zeran*[40] the court held

---

[35] See Mullooly, "Liability for Defamatory Statements on the Internet: A Comparative Overview", (2000) 2 *Hibernian Law Journal* 202.

[36] See, for example, the UK case of *Godfrey v. Demon Internet* [1999] E.M.L.R. 542.

[37] Mullooley, (2000) 2 *Hibernian Law Journal* 202, 203.

[38] One example of this would be the case of *Cubby Inc v. CompuServe*, [1991] 776F Supp 135. The case of Prodigy, however did hold the ISP liable as the court placed relevance upon the fact that Prodigy had held itself out to customers as being family friendly in that it exercised editorial control over content. *Stratton Oakmont v. Prodigy*, 932 MedLor, 1794 (NY SE) Nassau County, 1995.

[39] 47 USA 230 [1996].

[40] *Zeran v. AOL*, 129F.2d327(1997).

that Section 230 of the US Act prevented liability attaching to the ISP even when on notice. The *Demon*[41] case in the UK shows that ISP's currently have less protection under current UK (and Irish) law. The defendant ISP attempted to rely upon a defence under the Defamation Act, 1996 (UK) a defence akin to innocent dissemination.[42] Three elements must be established for the defence to arise, namely:

1. the (ISP) was not the owner, author, editor or publisher of the statement;
2. it took reasonable care in relation to its publication; and
3. it did not know and had no reason to believe that what it did, caused or contributed to the publication of a defamatory statement.

As the ISP had been put on notice by the defendant of the defamatory statements and did not remove them the defence could not be established. Mulooley points out that there is no comparable provision under Irish law to Section 1 of the Defamation Act, 1996 (UK).[43] A similar decision to *Demon* could be reached in this jurisdiction. Employers can be held vicariously liable for the acts of their employees while acting within the scope of their employment.[44] Both of these areas will continue to be litigated and depending on the nature of the publication this may involve electronic evidence.

I. Documents Under Seal

If a law requires a seal to be affixed to a document that requirement is met if the document includes an advanced electronic signature based on a qualified certificate of the

---

[41] *Godfrey v. Demon Internet* [1999] E.M.L.R. 542.

[42] Mullooley, (2000) 2 *Hibernian Law Journal* 202, 210.

[43] Mullooley, (2000) 2 *Hibernian Law Journal* 202, 210

[44] *Lloyd v. Grace Smith* [1912] A.C. 716, *Limpus v. London General Omnibus* [1861-73] All E.R. 556; [1862] 1 H & C 526. See Newman, "Evidential Issues", (2000) Law Society CLE seminar.

person by whom it is required to be sealed.[45] However, an advanced electronic signature based on a qualified certificate may only be used for this purpose:

1. where a public body consents and any particular requirements are met; and
2. where the person is not a public body that person consents to the use of the advanced electronic signature based on a qualified certificate.[46]

J. Electronic Originals

If the law or otherwise requires/permits the presentation or retention of information in its original form the information may be retained in electronic form. However for this to apply there must exist a reliable assurance as to the integrity of the information from the time first generated in its original form.[47] Integrity will be a matter of evidence to be adduced before the court. This may involve a company IT administrator giving evidence indicating that the particular computer systems involved were performing normally. No extensive indication is given in the Act in relation to the standard of integrity or whether the factors referred to in the Act are exhaustive. Courts therefore will have to examine the issue on a case by case basis. It is likely that the party opponents will also offer specialist witnesses in particular cases. The nature of such evidence may also be of a quite detailed technical nature as it can relate to the particular IT systems involved.

K. Retention and Production

If existing law requires information to be retained in its original form this requirement is fulfilled if the information is retained in electronic form subject to assurances in relation

---

[45] Section 16(1).

[46] Section 16(2).

[47] Section 17. This originally comes from Article 8 of the UNCITRAL Model Law.

to the integrity of the information from the date of its creation to the date in question so long as the information remains complete and unaltered. Similarly, there may be a requirement to produce evidence of an IT Administrator or an expert witness in relation to the electronic evidence.

L. Contracts

The Electronic Commerce Directive states that

> Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.[48]

An electronic contract under the Electronic Commerce Act shall not be denied legal effect, validity or enforceability *solely* on the grounds that it is wholly or partly in electronic form or has been concluded wholly or partly by way of an electronic communication.[49] Courts have previously accommodated certain technological developments. For example, contracts making use of the facsimile and the telex have been held to be valid and enforceable.[50] However the Act

[48] Article 9(1).

[49] Section 19(1). See also Article 11 of the UNCITRAL Model Law.

[50] See Murray, "The Electronics Commerce Bill, 2000", (2001) 11 *Irish Law Times*, 174 and 174 n. 5. However there is ongoing debate as to whether specific laws need to be enacted to accommodate technological advances. We previously saw this in relation to jurisprudence under the Copyright Act, 1963. A recent example shows that this debate is still ongoing. In *Random House v. Rosetta Books*, a Federal District Judge in New York ruled that the right to print, publish and sell works in book form in the contracts under consideration did not include the right to publish the works in electronic format. See Italie, "Federal Judge Reject Random House Request for Injunction Against E-Publisher", at

ensures that those transacting over the Internet can rely on these contracts with greater assurance.

In the formation of a contract an offer, acceptance or any related communication (including subsequent amendment, cancellation or revocation of the offer or acceptance) may, *unless otherwise agreed* by the parties, be communicated by means of an electronic communication.[51] Therefore, pre-existing contract principles may well continue to be relevant. Equally, collateral documentation (be it in paper or electronic form) can also be relevant. In addition the provisions in relation to acknowledgement and receipt of electronic communications will be pertinent. As noted previously, existing consumer law shall also apply to electronic contracts as will the remit of the Director of Consumer Affairs.[52]

M. Acknowledgement of Receipt of Electronic Communications

Under Section 20[53] of the Electronic Commerce Act there are provisions in relation to the acknowledgement and receipt of electronic communications. Where the sender of an electronic communication *indicates* that a receipt is required to be acknowledged but does not specify the particular form of receipt then unless otherwise agreed the acknowledgement shall be given by way of electronic communication or other communication (including conduct) sufficient to indicate to the originator the electronic communication has been received.

Sub-section 20(2) provides that if the sender indicates that receipt of the electronic communication must be

http://news.findlaw.com/ap_stories/1/0000/7-12-2001/20010712083008670.html, accessed on 16 July, 2001. New York District Court, Case No. 1:2001 cv 01728. See also http://www.thestandard.com/article/0,1902,22509,00.html.

[51] Section 19(12).

[52] Section 15.

[53] Sections 20 and 21 should be compared with Article 11 of the Electronic Commerce Directive.

acknowledged to establish a legal right then until the acknowledgement is received by the sender it shall be treated as if it had never been sent. Under sub-section 20(3) if a receipt is required but it is not stated that the electronic communication is conditional on the receipt of the acknowledgement and the acknowledgement has not been received within the time specified or a reasonable time then the electronic communication is treated as if it was never sent. This is similar to Articles 14 and 15 of the UNCITRAL Model Law.

N. Time and Place of Dispatch/Receipt of Electronic Communications

Article 11 of the Electronic Commerce Directive provides that Member States must ensure that the following rules apply when consumers place orders through technological means. These are that:

1. the service provider must acknowledge receipt of the recipient's order without undue delay and by electronic means;

2. the order and acknowledgement of receipt are deemed received when the parties to whom they are addressed are able to access them.

The Electronic Commerce Act also sets out provisions in relation to the time and place of despatch and receipt of electronic communications.[54] Where an electronic communication enters an information system, or the first information system outside the control of the sender, it is taken to be sent when it enters such a system.[55] If the addressee designates an information system for receiving electronic communications the electronic communication is taken to be received when it enters that information system.[56]

---

[54] Sections 20 and 21 should be compared with Article 11 of the Electronic Commerce Directive.

[55] Section 21(1).

[56] Section 21(2), unless otherwise agreed.

Where the addressee of an electronic communication has not designated an information system for receipt, the electronic communication is taken to have been received when it comes to the attention of the addressee.[57]

Unless otherwise agreed an electronic communication is taken to be sent from and received at, respectively, the place where the originator and the addressee have their place of business.[58] If they have more than one place of business the relevant place will be the place of closest relationship to the transaction or, if there is no underlying transaction, the place of principal business. If there is no place of business the place of business is taken to be the place where he or she ordinarily resides.[59]

O. Consent

The Electronic Commerce Act is premised upon the concept of consent. Section 24 indicates that nothing in the Act means that a person is required to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form. Neither shall the Electronic Commerce Act be construed as prohibiting a person or public body engaged in electronic transactions from establishing reasonable *requirements* upon the manner upon which the person will accept electronic communications, signatures or the electronic form of documents. Therefore it is up to individuals or public bodies to specify the particular circumstances and requirements upon which they will be prepared to accept and/or enter into electronic communications. Incidentally, a public body is defined in the Electronic Commerce Act to mean a Government Minister or Minister of State; a body

---

[57] Section 21(3), unless otherwise agreed.

[58] Section 21(5).

[59] This now should be read in light of S.I. No. 207 of 2001 on distance communications contracts. See also the Distance Contracts Directive, 97/7/EC 20 May 1997 [1997] O.J. L144.

funded out of the Central Fund; or a commission, tribunal, board or body established by an Act or by a Minister.

P. Privacy/Key Escrow

One of the main issues that any legislature introducing electronic commerce legislation has had to deal with was the issue of getting access to encryption keys. This is an issue which is still being widely debated internationally. Many law enforcement agencies, particularly in the U.S. and U.K., argue for a system of key escrow with trusted third parties (i.e. key escrow) so that they can access encrypted electronic communications as deemed necessary. The Irish legislation took a deliberate policy decision of not insisting on key escrow or key recovery but rather of ensuring the ability to acquire the encrypted message. In contrast, the UK adopted a position of requiring access to keys, an approach largely criticised by industry generally. The main difference between key escrow and key recovery is that the former involves disclosing the key details in advance of the creation of any messages.

Section 27 of the Electronic Commerce Act provides for disclosure of encrypted messages during certain investigative procedures. However Section 28 provides generally that "nothing in this Act shall be construed as requiring the disclosure or enabling the seizure of unique data, such as codes, passwords, algorithms, private cryptographic keys, or other data, that may be necessary to render information or an electronic communication intelligible." Murray[60] queries whether the liberal approach of the Electronic Commerce Act will have to be balanced against other laws such as the Child Pornography and Trafficking Act, 1998.

IV. General Comments

---

[60] Murray, "The Electronic Commerce Bill, 2000", (2001) 11 *Irish Law Times*, 174, 176.

A. Electronic Commerce Contracts

Given that more and more transactions will be conducted wholly or partly electronically, electronic evidence will be relied upon more progressively by litigants. One can argue that the formation of contracts electronically is no different from traditional methods of contracting. The formation of the contract still requires the same fundamental elements to be present, namely:

- an offer
- acceptance of the offer
- consideration, and
- an intention to create legal relations

When contracting electronically (particularly with consumers) one also has to consider the "information requirements" which apply under EU legislation. Certain information must be provided to consumers in advance of transactions. Under the Distance Contracts Directive[61] the recently enacted European Communities (Protection of Consumers in respect of Contracts by Means of Distance Communication) Regulations, 2001[62] and the Electronic Commerce Directive,[63] consumers must be provided with particular information prior to entering into the contract. This information includes identification of the (technical) steps required to conclude the contract, the name and identity of the service provider, VAT number, a procedure for correcting errors on the input screen as well as identifying particular choices of law.

Ultimately it is a matter of evidence as to whether the requirements have been satisfied. A general principle of contract law is that an individual is not bound by terms and conditions unless the terms have been incorporated into the

---

[61] Directive 97/7/EC 20 May 1997 [1997] O.J. L144.

[62] S.I. No. 207 of 2001.

[63] Directive 2000/31/EC 8 June 2000 [2000] O.J. L178.

contract. Typically, this means that the terms have been brought to their attention in advance of contract formation. Inevitably, disputes will arise as to whether an electronic communication of an offer or acceptance has been received and whether the information requirements have been fulfilled. Of critical importance will be the evidence that can be produced of the tracking or receiving of the information at a particular point in time.

One example of proving an electronic commerce transaction may involve the booking of an airline ticket. In proving the booking transaction the airline may need to adduce electronic records of the transaction. If these records are purely computer generated (as opposed to computer records created with human intervention) they are more easily admissible as no issue of hearsay arises.[64] Newman points out a procedural problem which may arise in Ireland in relation to electronic evidence. In the absence of something equivalent to UK practice and procedural rules of court in relation to advance notice of evidence, the defence may not be aware of the existence and nature of the electronic evidence to be produced by the airline nor, for example, of the need for expert rebuttal evidence.[65] Given the complexity and technical nature of some of the electronic evidence which parties will no doubt seek to rely upon, it may be worthwhile seeking to have similar advance notice provisions under the Irish court procedural rules. In addition, there may be situations where it may be worth considering the provision of a judicial discretion to appoint court experts.

---

[64] *R v. Minors* [1989] 1 W.L.R. 441. Note also the case of *R v. Shepherd* [1993] 1 All E.R. 225 and commentary by Reed, "Computer Records as Evidence – Back to the Beginning", (1993) *Journal of Business Law*, 505. This case related to a store detective giving evidence of examining till rolls in an attempt to prove that the items the defendant had in her possession were not paid for as no till receipt for that amount had been run through. See Newman, "Evidential Issues" (2000) Law Society CLE seminar.

[65] Newman, "Evidential Issues", (2000) Law Society CLE seminar.

B. Email and Electronic Copies

Email and electronic copies are discoverable and capable of being introduced in evidence. In fact a general order for discovery may well encompass electronic copies. The cost of actually producing these copies can be quite expensive depending on the particular organisation. For example email communication, both commercial and personal, is increasing in popularity and volume. It is estimated that by 2004, 272 million people will have email access at their place of work.[66] Electronic communications are being used to negotiate deals, transfer data, place orders as well as for private and public discussion. It is an interesting evidential point that evidence of electronic communications can often produce "smoking guns" because of its ease and casualness of use. In addition one can effortlessly "reply" or even "forward" emails to others. The forwarding of an email is noteworthy as traditionally to repeat a defamatory statement can amount to a new publication itself.

While there is a greater volume of communications there are now many more copies of each document. Every email can have six (or more) different copies at different locations. These are at:

1. the computer of the person sending the email;
2. the email server of the person sending the email;
3. the ISP of the person sending the email;
4. the ISP of the person receiving the email;
5. the email server of the person receiving the email; and
6. the computer of the individual recipient.[67]

---

[66] *IDC Predictions 2000 White Paper*, International Data Corporation, 29 March 2000, cited at Hart and Harrington, "In House Issues: Email, Internet Use and Document Retention, at http://www.plcinfo.com/scripts/article.asp?Article_ID=16121, accessed on 6 December, 2000.

[67] Menton, "Preparing for the Admissibility of Electronic Evidence in

Imagine how many copies there will be if one is sending an email to a number of people.

Companies increasingly have policies to safeguard against losing important data by means of regular backup copies. In an appropriate case one may wish to seek discovery of the "original" and backup copies. During the Iran-Contra affair in the US deleted emails between Oliver North and John Poindexter were retrieved from backup computer tapes.[68] The parties themselves were unaware that the communications could be recovered.

Voicemail can also be a source of pertinent electronic evidence. An interesting example concerned an employee of McDonald's who believed that his personal voicemail code was known only to himself. This was not the case as the employer also had access and the employer was able to listen to voicemails between the employee and his mistress. The employer played these messages for the employee's wife. A case was taken for breach of privacy but this eventually settled.[69]

Then, of course, viruses, trojan horses and worms (e.g. Melissa, I LoveYou, CodeRed) need to be considered. If a company forwards emails which contain viruses which damage the recipients computer system can the recipient sue? Furthermore can the plaintiff seek discovery of the company's Internet and email policy, for example, to see whether the policy states that the company claims ownership of all communications on the system e.g. "the system and everything on it whether transmitted or stored is the property of the company". If a defamatory statement is sent by employees acting in the course of their employment the

---

Court Proceedings", paper given at conference on *Legal Aspects of International E-Commerce* in Dublin, 10-11 May 2001, organised by Hawksmere.

[68] http://www.baker.com.hk/publicat/europe/alrt21/t-alrt21.html accessed on 10 March, 1998.

[69] http://www.baker.com.hk/publicat/ewope/alrt21/t-alrt21.html, accessed on 10 March, 1998.

plaintiff should be able to attach liability to the employer vicariously. Different considerations may apply if a contractor or consultant sends the email. Some companies require contractors as well as employees to sign Internet and Email policies. Some of these state that the company claims ownership of all content and communications on the system. Perhaps this could also be used as a means of seeking to attach liability to the company.

Defamation, viruses, loss of productivity, sexual harassment, leaks of sensitive commercial information, infringement and employee fraud are just some of the risks facing organisations. In *Western Provident Association v. Norwich Union* for example the defendants paid STG£450,000 damages in relation to defamatory internal emails. As Mulooley points out, however, the potential for damage is even greater in respect of Internet communication given its greater circulation.[70] She also refers to potential liability arising for universities for statements posted by students. Can liability arise in relation to defamatory statements posted by a hacker on a website? Mullooley suggests that a duty of care may arise. A duty of care may also arise if a website has been frequently hacked into (as frequently occurs) but the organisation has not increased its security measures. Many companies also seek to reduce their exposure by establishing Internet and Email use policies as well as monitoring policies. However, other issues such as privacy[71] and the expectation of privacy may then arise.[72] Some firms will also block all emails with file attachments,

[70] Mullooley, (2000) 2 *Hibernian Law Journal* 202, 209. Unreported apparently because of a High Court apology issued and a settlement of Stg£450,000.

[71] See *Halford v. The United Kingdom* [1997] 24 E.H.R.R. 523, which found in favour of the employee's expectation of privacy in relation to telephone calls. There were particular facts to this case which may limit its general applicability.

[72] The Data Protection Commissioner's 1999 Annual Report refers to employee complaints in relation to monitoring in the workplace. Annual Report of the Data Protection Commissioner (1999) 33.

while others use filtering software to block only certain email attachments entering their system.[73]

V. Future Issues

The *Verdi* case referred to above indicates that even when electronic evidence is admissible it ought not be relied upon without being adequately tested. Cross examination and even expert rebuttal evidence may be necessary to establish its veracity. Nicoll also points out[74] that an electronic "original" is often transitory and can be altered with ease. Different computer print outs may occur depending on the timing of the print request and this can be of "forensic importance". This also applies to the issue of "images" of computer memory. What if an "image" is not made *in situ* but rather the computer itself is taken. Who has access to it prior to the IT person subsequently making the image of the computer memory?

The extent to which evidence should be admitted and/or given weight also depends upon whether the technology in question is recognised as tried and tested.[75] For example Nicoll reports that in New Zealand computer devices have not yet achieved acceptable notoriety so as to be considered tried and tested. Instead expert evidence of the correct working of the computer system is required.[76] As shown in the *Verdi* case that electronic evidence exists does not necessarily mean that it is correct or that it is reliable. One problem with human fallibility is that we tend to accept something more readily simply because of its technological pedigree. What is clear however is that both legislative measures and advances in devices and communications

---

[73] Examples of such companies would include Network Solutions Inc. and the IE Domain Registry.

[74] Nicoll, (1999) *Journal of Business Law* 332, 338.

[75] Nicoll, (1999) *Journal of Business Law* 332, 340.

[76] Nicoll, (1999) *Journal of Business Law* 332, 340, citing the case of *Holt v. Auckland City Council* [1980] 2 N.Z.L.R. 124.

technology will increase the importance of electronic evidence.

Some of the particular types of electronic evidence we may see coming before the courts will relate to issues of contract formation and validity. This will also involve issues of who had particular information and at what time. Electronic evidence may increasingly become important in infringement and defamation cases. Discovery of electronic documentation will also become an increasingly popular avenue for litigants in particular factual situations. Electronic evidence may also become a familiar part of many criminal and civil forfeiture cases. In fact wherever litigation traditionally occurred there is now the potential for the applicability of electronic evidence. However considerations as to admissibility and reliability will remain. The increasing use of electronic evidence promises many changes to traditional litigation and court practices.