



5th BILETA Conference British and Irish Legal Technology Association

The Admissibility and Authentication of Computer Evidence - A Confusion of Issues

Chris Reed

Abstract: The Civil Evidence Act 1968 and the Police and Criminal Evidence Act 1984 set out requirements for the admissibility of certain types of computer-produced evidence. As part of the conditions of admissibility these statutes lay down minimum authentication requirements. However, the Acts arguably only apply to evidence that would otherwise be excluded as hearsay and not to direct or real evidence; in such a case the law contains no clear statements as to how that evidence should be authenticated.

The paper argues that admissibility and authentication are separate issues, and that the failure to treat them independently gives rise to needless confusion. This failure also directs attention away from the urgent need for clear rules governing the authentication of computer evidence. The lack of such provisions is a substantial obstacle to all types of digital communication and data storage.

Text

When in Dickens' *Oliver Twist* Mr Bumble opined that "The law is a ass - a idiot", it is certain that nothing was further from his mind than the digital computer. He was in fact referring to the presumption that a wife's actions are controlled by her husband. Had he known, however, that 150 years later English law would make assumptions about computer-related evidence that are at equal variance with the facts, his comments would probably not have been so temperate. In this respect the law today is as asinine as it is possible to conceive. Not only does it lay down conditions for admissibility which are both totally unnecessary and of Byzantine complexity (readers who doubt this latter assertion are directed to Tapper (1989) p.385 where the possible combinations of ss.2-5 Civil Evidence Act 1968 (CEA) are discussed at length), but it also fails to provide adequate rules for the authentication of this evidence. The result of this is that the development of electronic communications in commerce is seriously hampered.

1. Admissibility

There is not space in this paper to attempt a detailed exposition of the rules governing the admissibility of computer-related evidence, and in any event they are fully examined in a number of sources [Tapper (1989) Ch.9, Silverleaf & Reed (1990), Bradgate (1990), Reville (1989)]. If we are to examine their deficiencies, however, it is necessary to undertake a short overview of the law.

1.1 General problems of admissibility

Computer-related evidence falls into two clear categories. Each consists of information output by a computer, either as a result of some operation it has performed or as a hard copy of data stored in some permanent form (e.g. on magnetic disk). The first category is where the computer is used as a compact filing cabinet, in which are stored records of information provided to it by human beings. These records might be almost anything - observations of the weather, the serial numbers of cheques, notes of a meeting - but their essential characteristic for the purposes of admissibility is that they originate in an observation by a human. The second category consists of records generated directly by a computer, whether that which stores the record or another machine. Examples might be a system log for a mainframe installation, data received from a monitoring device such as a thermostat, or a record of an EDI (Electronic Data Interchange) message such as a purchase order produced automatically by a stock control system and transmitted to the supplier. Here the record is of an observation made directly by the machine without human intervention.

There are three reasons why a record produced by a computer might be inadmissible as evidence:

a. Because it is not an original. This does not appear to present any real problem in relation to computer records, as the original will in almost every case be a magnetically-stored version of the record which cannot be examined directly. Where the original is not available, the courts are prepared to admit properly authenticated copies [Reed (1989) pp.652-3].

b. Because it is hearsay. A document is hearsay if it is a record of a statement made by a human being of some fact which that human being has observed, or some action in which that human being has been involved. The reason for the hearsay rule is that the primary source of evidence in English law is oral evidence, given by a witness, of facts observed by that witness. In its original form the hearsay rule prevented a third party from giving evidence that the original witness claimed to have observed or taken part in some activity. This was because the second witness could not be cross-examined as to the truth of the first witness's observations. Documents falling within the first category outlined above will therefore be hearsay for exactly the same reason. However, a document that does not contain a record of such a statement is not in fact hearsay. If the computer document is a record of observations made directly by the computer, for example records of an ATM transaction, then it will not be hearsay but direct or real evidence. In general, direct evidence is admissible *per se*, though there is some debate whether this applies to computer records. This matter is dealt with below.

c. Because some rule of law prevents the evidence from being adduced. Some commentators have argued that all computer records fall within the definition of a statement in s.10(1) CEA and s.72(1) Police and Criminal Evidence Act 1984 (PACE) [see Bradgate (1990), Tapper (1989) p.403]. This provides that a statement includes "any representation of fact, whether made in words or otherwise". Computer records are clearly statements of fact and, so the argument goes, are therefore subject to the requirements of s.5 CEA or s.69 PACE, which prevent the statement from being admitted unless the conditions laid down in those sections are fulfilled. However, it should be noted that the courts have held that direct evidence produced by a computer is not subject to the hearsay rule [R v. Wood (1983), Castle v Cross (1985); see also The Statue of Liberty (1968)] and the Divisional Court has held in *Sophocleous v Ringer* (1988) that s.69 PACE does not apply where the computer has been used to calculate results, and thus produced direct evidence. This, together with the fact that the context of s.5 CEA suggests that "statement" means hearsay statement and that PACE uses the same definition, supports the view that the requirements of CEA and PACE apply only to hearsay statements [see Reville (1989) p.20, Silverleaf & Reed (1990) pp.180, 196]. Whatever the correct position, it is indisputable that the uncertainty is another factor militating against the effective use of computer communications.

1.2 Specific requirements for computer-related evidence

Where the computer records in question are hearsay, and possibly even where they are direct evidence, CEA and PACE set out a number of preconditions to admissibility.

Section 5 CEA provides that a statement in a document produced by a computer will be admissible to prove a fact so long as direct oral evidence of that fact would have been admissible and four further conditions are fulfilled. These conditions are set out in Section 5(2), and are as follows:

- "a. That the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activity regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;
- b. That over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;
- c. That throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and
- d. That the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities."

These four conditions show the age of the legislation. They are aimed primarily at the batch processing of identical transactions, and the type of computer operation envisaged by the legislature is clearly a substantial mainframe operation which is processing hundreds or thousands of similar transactions daily. However, the widespread introduction of microcomputers in recent years means that the types of information stored are far more diverse, and the regularity with which information of that type is recorded is less frequent, than would have been the case with mainframe systems of the mid-1960s. There is thus some doubt whether free-form databases or information contained in wordprocessed documents will, at least in precise terms, comply with these four conditions.

For criminal proceedings, s.24 Criminal Justice Act 1988, replacing s.68 PACE, provides that documents arising from trade, business, professional, occupational or official activities and which record information supplied by a person who has personal knowledge of the matters recorded are admissible in criminal proceedings provided the requirements of s.23(2) or s.24(4)(iii) are satisfied. Under s.23(2), the document is admissible if the person who would otherwise give oral evidence is dead or unfit to testify, if he is abroad and it is not practicable for him to testify, or if he cannot be found although reasonable steps have been taken to find him. Perhaps more importantly, s.24(4)(iii) permits the document to be given in evidence if the maker of the statement cannot reasonably be expected to remember the matters contained in the record. This section deals with the hearsay problem. It is important to note that, where a document is sought to be admitted under s.24, oral evidence must be given that the requirements of the section have been complied with [*R v Minors* (1989)]. This is in contrast to the accuracy requirements of s.69 PACE, which can be proved by certificate.

Even where a computer-stored statement fulfills the requirements of s.24 of the 1988 Act, it will not be admissible unless it also meets the provisions of s.69(1) PACE. These are (in paraphrase):

- a. that there are no reasonable grounds to believe that improper operation of the computer render the statement inaccurate;

b. that at all material times the computer was operating properly, or if not, that this does not affect the statement's accuracy; and

c. that any rules of court are satisfied. So far, no rules of court have been made under s.69(2).

These provisions are designed to overcome any doubts as to the accuracy of the statement, either because it was not stored correctly in the first instance or has become corrupt over time. This is not likely to be a problem with, say, a record of serial numbers which are input once and then stored until needed. However, if the computer is programmed to collate a number of separately input records (e.g. the various serial numbers of the component parts of a car) to make the record sought to be admitted, the court will need to be convinced that no inaccuracy has crept in during the processing of the data.

These matters may be evidenced by a certificate under para.8 of Schedule 3. The certificate must identify the document and describe the manner of its production, give particulars of the equipment used in its production, deal with the requirements of s.69(1) and purport to be signed by a person "occupying a responsible position in relation to the operation of the computer". It is sufficient for the certificate to be signed to the best of the knowledge and belief of that person. Para.9 gives the court power to require oral evidence of any of these matters, but it is unlikely to do so in practice unless the accuracy of the certificate is disputed. It was recently made clear by the Court of Appeal in *R v Minors* (1989) that computer records which are hearsay have to clear both these hurdles, and the mere fact that a record satisfies the accuracy requirements of s.69 PACE does not exempt it from the admissibility requirements of s.24 Criminal Justice Act 1988.

A critical examination of these admissibility requirements reveals that computer records, unlike other forms of evidence, are regarded as suspicious in two respects:

a. The technology for storing and processing data is believed to be inherently inaccurate. Both s.69 of PACE and s.5(2)(c) of CEA require some minimum proof of accuracy before the record can be examined by the court. The assumption is that not only must the court be satisfied of the reliability of the statement as a true record of what the witness observed, but also of its authenticity as an accurate record of what was intended to be recorded. Parliament envisaged that there would be many cases where the document might have become corrupted by software errors or hardware malfunctions. For these reasons it was necessary to show that at all material times the computer had been functioning properly, or at least that any malfunction had not affected the accuracy of the information. This suspicion was probably unfounded even at the time of the legislation; it is certainly the case today that a computer record is likely to be at least as accurate as one maintained on paper. This seems to have been recognised in practice, as the accuracy requirements are normally proved by the production of a certificate emanating from a responsible person in relation to the computer system, and that person is only required to certify the matters in question to the best of his knowledge and belief. Nonetheless, there is a substantial degree of uncertainty amongst computer users as to whether their computer records will be attacked on this ground by challenging the certificate [Castell (1987)]. If such an attack is made it will be necessary for the person issuing the certificate to give oral evidence as to the working of the computer. In many cases it is unlikely that the available information about the operation of the computer system will be sufficient to satisfy the court that the record has not been altered or corrupted. This uncertainty is delaying the introduction of computer systems to perform transactions which have potential legal significance (e.g. for contract formation under EDI).

b. The wording of s.5(2)(a), (b) and (d) CEA clearly assumes that the record to be adduced in evidence is a record of human observations, probably entered into the computer by a different person from the observer. It also assumes that information processed by a computer will normally be highly structured and consist of quantities of similar records, and that information

which does not possess these characteristics will have been processed by ad hoc and ill-tested software and for this reason be potentially inaccurate. In 1968, given the cost of mainframe software and its comparative difficulty of production, this might have been a valid assumption. That is untrue today, both in respect of the type of information stored on computers and its processing. The case for restricting the admissibility of computer-related evidence to accurate records is at least arguable, but if these conditions were strictly applied they would exclude records whose accuracy is not in doubt.

On any rational assessment of the problems in this area, authentication should go to the assessment of the weight to be attached to the record, rather than its admissibility. The confusion of authentication with admissibility can lead to erroneous decisions (the classic example is *R v Pettigrew* (1980)) and act as a brake on the introduction of new technology. As Tapper points out,

"There is no intrinsic reason why different regimes should apply to different forms of record-keeping, and every reason why they should not when the different forms are not readily distinguishable upon their face. There may be no obvious difference in appearance between a document produced by a computerised word-processing system and one produced by a manual typewriter, nor is there the slightest justification for subjecting them to different hearsay rules. To do so creates nothing but anomaly and confusion." [Tapper (1989) p.395]

2 Authentication

These defects in the rules of evidence, confusing as they do admissibility and accuracy, detract attention from the real difficulties which arise in relation to the authentication of computer-related evidence. It is important to understand here the issues that are at stake.

2.1 Authentication in theory

Authentication means satisfying the court (a) that the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features of the system or the record. Nontechnical evidence will include a wide variety of matters:

"In an ideal world, the attorney would recommend that the client obtain and record countless bits of evidence for each message so that it could later be authenticated in court - autographs, fingerprints, photographic identification cards, attestations from witnesses, acknowledgments before notaries, letters of introduction, signature guarantees from banks, postmarks on envelopes, records of the return of acknowledgments and so forth [These] observations on conventional messages should apply equally to electronic messages." [Wright (1990) p.80]

Technical evidence might come from system logs, particularly if they are specifically designed with this end in mind [Urbach (1985), Reed (1989) pp.655-6], or through embedded features of the record itself such as digital signatures [Longley & Shain (1987), Beckett (1988) Chs. 9 & 16]. I have argued elsewhere that these techniques will be acceptable to the courts as evidence of a record's authenticity [Reed (1989)], and indeed some US courts have taken a relaxed approach to the authentication of computer records, refusing to exclude computer-related evidence merely because corruption or alteration is theoretically undetectable [*US v Vela* (1982), *US v Sanders* (1984)].

2.2 Authentication in practice

This legal analysis does not dispose of the authentication problem, however. Academic authors and conference speakers may assure their audience that technical authentication is possible, and that the courts are likely to accept that technical authentication for evidential purposes, but no commercial enterprise is going to run the risk of lengthy and expensive litigation as a result. Only if the gains outweigh the risks will enterprises go over to fully automated systems of data storage and communication. This is clearly apparent from an examination of key areas of commercial activity.

2.2.1 *International trade*

The biggest problem facing importers and exporters is the distressing tendency of goods to arrive before the documentation which is necessary to ensure their release. Without the shipping documents the carrier will not hand over the goods and the bank will not release the funds for payment; without the customs declaration the customs authorities will refuse to clear the goods. This problem can be overcome by using computer technology to transfer the necessary information [Wheble & Thomsen (1989), Walden (1989)], but banks and, in particular, Customs authorities insist on physical documents precisely because of their doubts about the acceptability of electronic records as authenticated evidence. Customs are the biggest barrier, as they have no commercial incentive to take risks. It is clear that they will not accept electronic customs declarations without legislation providing for their use as evidence in legal proceedings [Morris (1989)]. Authentication is thus the biggest legal barrier to increasing the efficiency of international trade.

2.2.2 *Banking*

The major banks, and increasingly the building societies, have been forced by the sheer volume of documents and their associated costs to introduce computerised data storage and Electronic Funds Transfer (EFT). However, the potential risks involved are reduced by the special rules of evidence for bank records contained in the Bankers' Books Evidence Act 1879. Where the records amount to bankers' books, authenticated copies are admissible as *prima facie* evidence of what they state under s.3, and this authentication is effected by oral evidence or a certificate emanating from a responsible person. It is thus for the other party to raise doubts as to their authenticity. A "banker's book" is defined in s.9 of that Act, as amended by Sch.6 Banking Act 1979, to include ledgers, day books, cash books, account books and other records used in the ordinary business of the bank, whether in written form or recorded electronically. Even so, banks preserve vast quantities of paper such as paid cheques and deposit slips, in case such a challenge is mounted.

The level of technical authentication in EFT systems depends very much on the perceived risks. The SWIFT (Society For Worldwide Interbank Funds Transfer) system, which transmits more than 1 million messages daily, uses the RSA encryption method to authenticate these messages with an extremely high degree of security. This requires special hardware and software and complex procedures, and is accordingly very costly. By contrast, consumer EFT systems use simpler encryption technology (probably DES in most cases) and authenticate customer messages by using four-digit Personal Identification Numbers (PINs). The potential insecurity of this system is beginning to be appreciated [Cornwall (1990), Jack (1989) Ch.10], and it is worthy of note that the contractual terms governing payment and cash withdrawal cards generally throw at least some of the risk on the customer [Jack (1989) Appendix F].

2.2.3 *EDI and contract formation*

Computerised stock control and "just in time" ordering offer potentially large savings to industry.

They also require automatic ordering of supplies through EDI. This means that the evidence of contract formation lies solely in the electronic messages automatically generated by the seller's and buyer's computers. Until there are clear legal rules as to how far these contracts will be enforced by the courts, industry is reluctant to install such systems. In general it is only pressure from large customers, for whom the savings are substantial and whose bargaining power is such that they are confident of resolving disputes without recourse to litigation, that forces smaller manufacturers into using EDI.

2.3 The CEA and PACE as authentication measures

It should be clear from the analysis above that CEA and PACE at best address only the first of the three requirements for authentication set out in 2.1. Indeed, they only address part of that requirement, for a record can change without any system malfunction or improper use of the system, e.g. if it is amended over time to take account of new information, thus overwriting the original contents. Nothing in those statutes assists computer users in deciding how best to link the record with its maker, a role traditionally performed in relation to physical documents by an autograph signature. Nor, particularly if the record emanates from another computer, is there any provision which will assist in proving when it was sent, and from where. These matters are important in commercial transactions; but obviously not important enough to merit legislation.

3. Conclusions

It is time for s.5 CEA and s.69 PACE to be abolished. Special rules for the admissibility of computer-related evidence can no longer be justified, particularly where those rules are based on false assumptions about the technology. It is also time to legislate for authentication. Important questions need to be answered. Can an electronic document be "signed", and if so what will constitute a signature? Can the parties to a communications network agree authentication procedures which will then be accepted by the courts? Is a system log adequate evidence of the changes made to a record, and if so what should it contain? It is beyond the scope of this paper (and indeed the competence of the author) to put forward a draft Bill at this stage, but the longer work on this topic is delayed the worse the position will become.

Some might argue that a gradualist, case-based approach to reform will identify the real issues and produce better law. Such a "laissez faire" attitude is an inadequate response to these problems. The tradition that the law lags 10 to 15 years behind technological development will not produce the guidance which industry and commerce require if they are to compete in an increasingly international market. Indeed, the pace of technological change is so fast that the law is likely to fall further and further behind commercial practice. In the meantime uncertainty and confusion rule. Systems are not adopted, or (perhaps worse) are introduced in parallel with what may turn out to be unnecessary duplicate records, a sort of "belt and braces" approach which imposes heavy financial burdens and inefficient and cumbersome procedures.

It is necessary that the law should give a lead. Industry and commerce require clear guidance on how to make their records acceptable to the courts. Until this guidance is forthcoming, the law will indeed remain "a ass".

Books and articles

BECKETT B., *Introduction to Cryptology*, Blackwell Scientific Publications (Oxford 1988)

BRADGATE R., *The evidential status of computer output and communications* (1990) 6 Computer Law & Practice (forthcoming)

CASTELL S., *VERDICT report* (1987)

Cornwall H., *Datatheft*, Mandarin (London 1990) Ch.4

JACK, *Banking Services: Law and Practice Cm 622* (the Jack Report), HMSO (1989)

LONGLEY D. & SHAIN M., *Data & Computer Security: dictionary of standards, concepts and terms*, Macmillan (London 1987)

MORRIN J., *Customs requirements and international trade*, (1989) 6 Computer Law & Practice 42

REED C., *Authenticating Electronic Mail Messages - some evidential problems* [1989] MLR 649

REVILLE N., *The admissibility of computer statements in criminal trials* (1989) 6 Computer Law & Practice 19

SILVERLEAF M. & REED C., *Evidence in Reed* (ed.) Computer Law, Blackstone Press (London 1990) Ch.9

TAPPER C., *Computer Law* (4th Ed.), Longman (London 1989)

URBACH A., *The Electronic Presentation and Transfer of Shipping Documents* in R.Goode (ed.), *Electronic Banking: the Logal Implications*, Institute of Bankers/Centre for Commercial Law Studies (London 1985) p.111

THOMSEN H. & WHEBLE B., *Trading with EDI: the Legal Issues*, ESC Publications (London 1989)

WALDEN I.(ed.), *EDI and the Law*, Blenheim OnLine (London 1989)

WRIGHT B., *Authenticating EDI: the location of a trusted recordkeeper* (1990) 6 CL&P 80

Cases

Castle v Cross [1985] 1 All ER 87

R v Minors [1989] 2 All ER 208

R v Pettigrew (1980) 71 Cr App R 39

R.v Wood (1983) 76 Cr App R 23

Sophocleous v Ringer [1988] RTR 52

The Statue of Liberty [1968] 2 All ER 195

US v Vela 673 F 2d 86 (1982)

US v Sanders 749 F 2d 195 (1984)