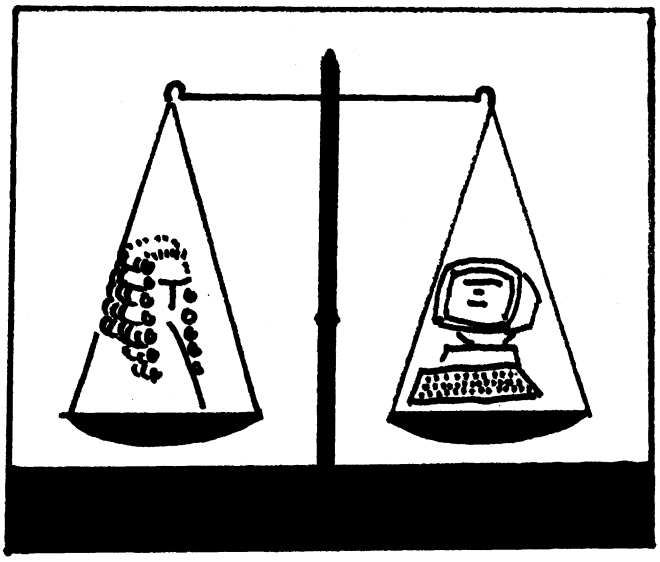
ARTICLES

WHAT IS COMPUTER EVIDENCE?



The Australian Law Reform Commission recently published Research Paper No.3 on Evidence, which particularly presented proposals on hearsay evidence to apply to business records kept in or by computers. Basically the proposal follows the rules for admissibility of business records on paper. If the data are entered as a normal business procedure with the item about which evidence is to be produced treated the same as any other then (see p.148) a printout of the item should be acceptable as an exception to hearsay evidence rules, subject to proof.

The proving suggested (p.154) is essentially to have an independent technical expert testify to the validity of the process of printing out the information. Other forms of proving records which are discussed included date stamps as in postmarks, and (in Research Paper No.10) the extent to which judicial notice can be used to accept evidence.

The objective of this short article is to illustrate some of the problems of establishing validity of computer records and reports from the viewpoint of the computer professional. Some extensions are suggested for the proving process.

Input documents

As discussed later under "Audit trails", it may be possible to prove output back to the original input document. Such an approach essentially assumes that there is an original document which can be verified as having been provided by someone other than the organisation wishing to present proof.

However consider these two scenarios:

1. The computer system is on-line. The one party rings up, and gives information verbally to the keyboard operator who enters it directly;

2. There is a document which purports to come from outside the organisation, and is used to provide input data. The document has been produced by wordprocessor or computer.

In the first instance the organisation could maintain it had entered information correctly but the second party could claim to have said something different. Several ways are possible from a computing viewpoint to solve the validity problem, including voice recording all such messages and using an echo check in which all input messages are printed and despatched to the originator for verification. Without some form of message authentication by sender and receiver it will always be difficult, if not impossible, to establish the truth.

In the second case, the originator could send one printout to the organisation as a source document, while then (or previously) editing it to show different details and/or dates, and printing *that* out as the record of what is claimed to have been sent. There is no way for anyone to distinguish between the two printed versions as one being original and the other a copy or modification. Time and date stamps are of no value as these are usually fed into a machine and can be altered without trace.

The machine produced document could be copied to a diskette and removed to another location where it is modified and printed. The initiator of the transaction could maintain that he was not responsible for the particular input and there would be no evidence either way of the theft, although there might just be a witness to the printout. This is similar to manual fraud by a clerical officer inserting a form into a checked batch of input documents.

Derived data

The data which are printed out in a report need not be the original input. Computations may be made on input data and only the calculated values kept. A simple example is the summation of individual sales invoices to provide total sales and value by product. In large scale systems it may be possible to keep the detail level transaction for some time, but most microcomputer systems tend to keep only a month's transactions and summarise, for instance, to a general ledger account.

By the time the information is printed out, supervised by an expert, only the derived data may be present. The expert would, unless considerable effort is spent examining records of changes, which few organisations now keep, be unable to say whether the data were correct or not. It may not be possible to determine whether an invalid program had been used or what the original data had been.

Some control techniques are possible for auditing this type of risk. They would include the expert bringing into the organisation a validated copy of the supposed program and showing that the derived data can be produced from the supposed input data. They can also include in-line tests where specific data are fed in from time to time and output verified as that expected. An unerasable audit trail would be needed for the expert to inspect, to be satisfied that input and derived data are correctly related.

Even then it may be possible to produce the same output from different input. The number ten can be derived by adding six to four, or adding three to seven. Further, an amount of $100 paid to Mr Brown will add into a grand total in the same manner as $100 paid to Mr Black.

Derived data cannot therefore often be used to establish what occurred unequivocally. The best that could be said is that the derived data are consistent with some claimed input.

Mutability

The major concern to the comuputer person is the ease with which data can be modified. A printout may be valid as a statement of what is recorded in the system at the time of printout. Even if the data is alleged to be unchanged, there is no guarantee that the printout reflects what was initially entered.

Sources of change may be programming errors in the initial recording, accidental changes when two valid users gain access to a record, deliberate change to the recorded dates using special programs or so-called utility programs to be found on all computer systems. Only in very exceptional cases would it be possible to detect that the change had been made.

Only when an unerasable audit trail, which must always be used, exists could any statement be made. However, as in the case of the Bank of England employee who had to enter serial numbers of supposedly destroyed banknotes, the "proof" of validity would require the absence of a change record. Such evidence has been rejected in the past, and, with present audit trail techniques, should remain rejected. The absence of a changed record may mean no change, or may mean that someone has deleted the relevant audit trail record and rearranged the audit trail file to show no physical gaps and continuity of sequence numbers and time stamps.

Audit trails and access control

Proof of the presented data may therefore have to extend to the expert witness testifying to the ability of the organisation's control mechanisms to minimise the risks outlined and thus on the balance of probabilities there is a correspondece between output and initial input.

The major control tools for this purpose would be the audit trail which separately records each event that occurs in chronological order, and control of access.

The law might have to insist on some unerasable medium for an audit trail to feel confident enought to accept it. Costs of such a device would, in general, militate against its widespread use.

Access controls can be used to restrict access to programs and data to specific persons and possibly with other restrictions such as reading data with a specific program, or use at a particular time of day or from a particular terminal. Such systems are quite sophisticated and are, at present, only found on large scale systems. Mini or micro computers may have relatively primitive password schemes, but they should really be considered uncontrolled.

Conclusions

The approach suggested by the Law Reform Commission would not work. So-called expert testimony would not be in a position to say other than what is or was recorded at the time of printout.

Some progress could be made though requiring also that the controls on the system (audit trails, access controls, error detection, usage synchronisation and so on) were both in place and effective at the time of the alleged incident.

Even so it would be a brave or foolhardy computer expert who would swear that printed output truly reflected what was fed in. There are too many ways for accidental or deliberate change to occur without leaving a trace.

* Dr L.G. Lawrence
Freelance Computer Consultant
Vonaldy Pty Limited