The *Evidence Act* 1995 (Cth): Should Computer Data Be Presumed Accurate?

LYNDA CROWLEY-SMITH*

INTRODUCTION

On the 18th of April 1995, the *Evidence Act* (Cth) [hereinafter referred to as 'the Act'] came into force in Australia. It is the product of sixteen years of work through the combined efforts of the Australian Law Reform Commission and some of Australia's leading lawyers to include 'several novel features'.[1] The *Act* consists of 197 sections about the law of evidence and related purposes. It is in most respects uniform with the *Evidence Act* of New South Wales.[2] Except for minor annotation and drafting variations consistent with the fact that one is a Commonwealth Act and the other is a State Act, both pieces of legislation are said to be drafted in identical terms.[3] Other Australian States and Territories also contain provisions relating to the admissibility of computer records in their respective legislation.[4] Although different approaches have been adopted by the various jurisdictions, an analysis of the differences is beyond the scope of this paper. Suffice it to say that the Minister for Justice, Mr Kerr, encourages all the States and Territories 'to follow the lead of the Commonwealth and the Australian Capital Territory and to adopt the reforms contained in the Act'.[5]

The Act contains a number of new provisions providing fundamental changes to the law of evidence. One of its aims is to bring the rules of evidence in pace with rapidly changing computer technology and information processing systems. This is to be achieved by allowing into evidence documents and business records generated from computer stored information.

This paper is concerned with the provisions that modify the rules of evidence in an attempt to cope with the new technology of computers. In the absence of credible evidence to the contrary, certain things are now presumed as evidence in Australian federal courts. For example, there is now a presumption of working accuracy in relation to computers and their software. In some cases, the requirement to produce the original document in federal court proceedings has been abolished. Further, there are exceptions to the hearsay rule concerning telecommunications. The focus of this paper is to highlight some of the dangers involved with provisions such as ss 71, 146 and 147,

* LLB (QUT); Barrister, Supreme Court of New South Wales; Lecturer, Business Law, James Cook University of North Queensland. I am indebted to Chris Linfoot for his comments.

1 D Kerr, Minister for Justice, 'Foreword' in G Bellamy and P Meibusch, *Commonwealth Evidence Law with Commentary* (1995), iv.

2 *Evidence Act* 1995 (NSW).

3 *Evidence Act* 1995 (Cth).

4 *Evidence Act* 1977 (Qld) s 95(1); *Evidence Act* 1929 (SA) s 59b(1); *Evidence Act* 1958 (Vic) s 55B(1).

5 Kerr, op cit (fn 1) iii.

which permit assumptions about the accuracy of evidence produced or processed by information processing systems.

THE PROVISIONS

The Act refers to several provisions that specifically relate to the admissibility of electronically produced information.[6] Pursuant to s 71, it is assumed that an electronic data interchange (EDI) message log, such as that accompanying an electronic mail message or fax, accurately records transactions between parties. For instance, it is presumed that certain data such as the date time stamp,[7] and the identity of the sender and the receiver,[8] are accurate. A fax is now regarded in evidence as good as the original.

More specific provisions relating to computer information may be found in Part 4.3 of the Act. Section 146 applies to 'documents or things produced by processes, machines and other devices'[9] and s 147 applies to 'documents produced by processes, machines and other devices in the course of business'. Central to the reforms is the concept of 'document'. The word 'document' is broadly defined in the Act's Dictionary as any record of information including anything on which there is writing, marks or figures which can be interpreted and images or writings which can be reproduced with the aid of anything else.[10] According to the Law Reform Commission, the definition includes all methods available for storing information including computer disks, computer tapes and the like.[11]

It is proposed by s 146, that where it is reasonably open to find that a 'device or process'[12] is of a kind that, if properly used, ordinarily does what it is claimed to do, the court shall presume that the particular device or process did, on the occasion in question, produce the document or 'thing' unless there is sufficient evidence to raise doubt about such a presumption. The Law Reform Commission, in its Interim Report, *Evidence*, states that the provision removes doubt about machine produced evidence.[13] Thus, evidence as

[6] For example, *Evidence Act* 1995 (Cth), ss 71, 146, 147.
[7] Id s 71(b).
[8] Id s 71(a), (c).
[9] Id s 146:
(1)This section applies to a document or thing:
(a) that is produced wholly or partly by a device or process; and
(b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.
(2) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question the device or process produced that outcome.
[10] Id Dictionary, 93.
[11] Australian Law Reform Commission, Report 26, *Evidence* Vol 1 (1985) 285.
[12] Id 551. According to the Law Reform Commission, the expression will cover computers and their software.
[13] Ibid.

to the working accuracy of a particular device or process is no longer required.

Section 147 specifically deals with the production of 'business records'. The section in part is as follows:

(1) This section applies to a document:
  (a) that is produced wholly or partly by a device or process; and
  (b) that is tendered by a party who asserts that, in producing the document, the device or process has produced a particular outcome.
(2) If:
(a) the document is, or was at the time it was produced, part of the records of, or kept for the purposes of, a business (whether or not the business is still in existence); and
(b) the device or process is or was at that time used for the purposes of the business;
it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document on the occasion in question, the device or process produced that outcome.

The term 'business' is widely defined in the Act's Dictionary. It includes a profession, calling, trade, a non-profit business, a foreign business or government activity, the committee or proceedings of an Australian Parliament or a House, or the committee or proceedings of a legislature of a foreign country or House.[14]

Sections 146 and 147 share similarities. Both deal with documents produced wholly or partly by a device or process. Section 147 proposes that where a business document was produced by a particular device or process used for the purposes of that business, the court shall find the particular device or process accurately produced the document, unless on the occasion in question, there is sufficient evidence to raise doubt about the presumption. Put simply, business records stored and produced from a business data base are presumed accurate. As with s 146, evidence as to the working accuracy of a particular device or process in producing documents is no longer required.

However, there are also discrepancies. Section 146 applies to a 'thing' and unlike s 147, is not limited to business records. Under s 147, the device or process which produced the business record must be, or have been at the relevant time, used for the purposes of the business. The section does not contain the threshold prerequisite found in s 146 (2) that it is reasonably open to find that the device or process if properly used, ordinarily produces the outcome.

Finally, there is a proviso in s 147 (3). The subsection negates the presumpduced after the instigation of proceedings[15] or made in connection with a criminal investigation.[16]

[14] *Evidence Act* (Cth) 1995, Dictionary, Part 2, 96–7.
[15] See s 147(3)(a).
[16] See s 147(3)(b).

The subsection appears ambiguous. It does not allow the contents of a business document to be presumed accurate if it was produced for the purposes of, or in contemplation of, or in connection with any proceedings. Thus, the contents of a document that was produced any time prior to any such proceedings is presumed accurate pursuant to subsection (2). This places great significance and emphasis on the term 'produced'.[17] The word is not defined in the Act's Dictionary or within the relevant provisions. It is unclear at what point the legislation considers the production of a document to be complete. The ordinary dictionary meaning of the term is of limited assistance.[18]

Three possibilities emerge. It is arguable that production occurs when information is keyed into the computer and saved. It is also arguable that production, for the purposes of the Act with regard to the admissibility of electronically produced business records, occurs when the document is printed-out. Then again, it may mean when the document is produced in court. Since the presumption of accuracy depends on when the contents of the document were produced, it is imperative that the term 'produced' is clearly defined.

ERROR SOURCES AND THE RELIABILITY OF COMPUTER PRODUCED EVIDENCE

The statutory provisions in the *Evidence Act* which recognise computer generated documents as evidence are overdue and welcome. However, they do not take into account the accuracy of source data itself and errors propagated through systems. For example, the accuracy of data bases depends on the accuracy of the information which has been entered into them. According to Stamper, all data transmissions are subject to error.[19] The reliability of systems is said to have been a major concern since the beginning of the electronic digital computer age.[20]

Although the devices used to produce business records such as computers, disks, printers and the processes or programs involved may all be working properly, if the data in the system is incorrect the report produced by the device and program will also be incorrect. In order to determine whether computer processed information is accurate, it is necessary to understand how computing systems fail. A fault can be caused by physical failure, a system or design flaw, environmental influence or by the system operator.[21]

[17] See s 147(3).

[18] *The Australian Concise Oxford Dictionary* (1987), 873, includes in its definition of produce: 'bring forward for inspection or consideration; bring before the public; extend; continue; manufacture from raw materials etc.; bring into existence...'

[19] D A Stamper, *Business Data Communications* (3rd ed, 1991), 93.

[20] R A Maxion, D P Seiwiorck and S A Elkend, 'Techniques and Architectures of Fault-Tolerant Computing' (1987) 2 *Annual Review of Computer Science* 469.

[21] Id 473.

More than 30 per cent of system crashes are caused by human error[22] and as many as 70 per cent of failures in electronic equipment are human initiated.[23] Every user is a novice at least to some degree with respect to some computing system. As computer technology continues to evolve, the typical user becomes less knowledgeable about the system.

Daily errors, other than those created by human intervention also occur within computer systems and through the transmission of data. Although the aim is to achieve fault free devices or fault tolerant computing, this goal has not yet been fulfilled. For example, the log created by a fax, e-mail transmission or telex may not be accurate if the message is sent or received on a device or personal computer which does not have the correct date or time on its clock. Personal computers are not necessarily synchronised. A program, however, can be installed which does synchronise the clock to the mainframe clock which is in turn synchronised to the atomic clock in France. Such a program reduces this type of error.

Other than the internal working of the machine there are numerous forms of external influences which affect data and electronic processing systems. Electromagnetic forces such as lightning, sunspot activity, power surges, large magnetic fields in the general environment, white noises and crosstalk are capable of altering the operation of programs within devices and lead to transient faults.[24] The difficulty with transient faults is that they do not result in physically damaged hardware so repair is impossible.[25] Maxion states 'in the hierarchy of failures, physical defects are at the lowest level'.[26] Physical defects, such as some semiconductor chip failures, result from manufacturing defects. Other failures are a result of stress during normal operation.

Devices are not fault free either. The hard disk inside an ordinary computer has an approximate life of between three to five years. After that time their failure rate escalates and the risk of data becoming altered is consequently enhanced. As failures increase so too do the changes which may occur to the information held in data bases. At first, there may be subtle changes which cannot be detected but which the computer is capable of rectifying. Then, there are more severe and obvious changes to the data which again may be detected by the computer. There may also be catastrophic changes which result in the loss or alteration of data and which are not identified by the computer system. Fault tolerance is attempting to reduce this problem. The primary goals of fault tolerance is to avoid downtime and ensure correct operation even in the presence of faults.[27]

The Act further raises the issue of the shelf-life of optical disks. The question to be considered is how long will the digital version stay intact if the original paper-base evidence is shredded. Quite simply, no one knows. Com-

[22] Id 511.
[23] Ibid.
[24] D F Halsall, *Data Communications, Computer Networks and OSI* (2nd ed, 1992) 93; Stamper, op cit (fn 19) 94; Maxion et al, op cit (fn 20) 474, defines transient faults as 'a fault error resulting from temporary environmental conditions'.
[25] Maxion, loc cit (fn 20).
[26] Id 475.
[27] Id 472.

puter tapes have been used to store information for years. The tape is made up of a polymer strip which has on it magnetised iron particles. The orientation of the particles is the data, and that is how it is stored. The tape itself is stored as a reel which means there is close contact between each layer. Given they are magnetised, one magnetic field may affect another field due to proximity. Therefore over time, data can be altered without any outside interference whatsoever. Even if the tape is stored in a magnetic and humidity free environment to prevent deterioration of the tape itself, data may still be changed.

Today, optical disks are purported to take over tape storage but again no one knows how long stored information will last. Given that the disk does not physically come into contact with any other device such as a tape head, because the reading device is a laser light, the assumption is that the laser technology will prove better than tape in terms of accuracy and longevity of data storage.

Care must also be exercised when assuming an electronically produced image is correct when presenting it as evidence. Computer stored images can easily be changed intentionally by people. They can also be unintentionally changed by the simple use of different devices. For example, when printing an image from a personal computer the printer and the process may be working correctly, but by the very nature of the process, a degraded image could result when printed. This is because most computer screens have higher resolutions than many printers. Similarly, laser printers have higher resolutions than bubble jet printers and so on. Thus, the image produced by a laser printer may be more accurate than the same image produced by a bubble jet printer.

The Supreme Court of Tasmania was placed in the precarious position of having to determine whether computer produced evidence was admissible in *Maynard's* case in 1993.[28] In that case, Wright J, on an appeal by way of notice to review, held that the magistrate, during the hearing at the Court of Petty Sessions in Hobart, had erred in law. The magistrate had ruled that several sheets of hard copy print-out purporting to show times and dates upon which the respondent, an employee of the Department of Social Security, unlawfully accessed information stored in a computer owned by the Department relating to the personal affairs of various persons, were inadmissible evidence. His Honour found that computer-generated documents such as trace print-outs, as compared to a print-out of a bank statement, are admissible as real evidence.[29] Unlike a print-out of a bank statement which relies upon the accuracy of a number of operators who record transactions, Wright J said 'the process now under discussion is, as I see it, totally devoid of any such human hearsay element'.[30]

Following a demonstration of the computer tracing process, the magistrate had found that the document in question did not accurately portray the information that may have been displayed on the computer screen.[31]

[28] *Maynard* (1993) 70 A Crim R 133.
[29] Id 143. Wright J refers to the headnote in *Wood* (1982) 76 Cr App R 23 (CCA).
[30] Id 141.
[31] Id 136.

Wright J agreed that a computer may have been inaccurately programmed or operated and its mechanical componentry may be flawed or have broken down, but he said:

> If these inadequacies are suspected they may be probed by cross-examination of the program designer and operator or evidence may be called from other experts to demonstrate the shortcomings which are claimed to render the computer's end product valueless or of doubtful worth. If it withstands this scrutiny there appears to me to be no sound basis for concluding that any part of its function may be characterised as or equated with hearsay evidence.[32]

His Honour held that the computer system in question was a scientific device which, when properly used, was capable of and likely to produce reliable and accurate information of the kind in fact produced in the trace print-out.[33]

Although *Maynard's* case was an application of the common law, it is of concern that similar conclusions may be drawn by lawyers and by courts when applying the provisions of the *Evidence Act*. No independent checks were undertaken in *Maynard's* case to ensure the logical integrity of the trace program.[34]

Due to the myriad of errors which can and do exist in computer based systems, it is arguable that the rebuttable presumptions in ss 146 and 147 are misplaced. Instead, it is suggested with respect, it would be more cautious to replace the presumption with wording similar to the threshold requirement in s 146 (2) which in part states:

> If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, and that in producing the document or thing on the occasion in question, the device or process produced that outcome.

By providing a test of reasonableness it would be open for the court to find that the document or thing produced by a given device, process or machine was accurate unless sufficient evidence is admitted to raise doubt about the accuracy of such document or thing.

CONCLUSION

There are numerous benefits to be derived from the presumption of accuracy of computer data. Our current dependence upon computing systems has grown to such a point that our laws must progressively acknowledge their

[32] Id 142.
[33] Id 140.
[34] Logical errors often referred to as 'bugs' are discussed by E Guay, *Programming in Vax-Basic* (1987) 132, where he explains, 'logical errors do not produce error messages but cause the program to produce erroneous results. This kind of error can result from mistakes such as the incorrect use of a formula, the improper spelling of a variable name, or the use of faulty logic in your algorithm'. G Greenberg, *Vax Basic Programming* (1991) 86 where the author says, 'a program may be free from syntax and execution errors, yet it may produce incorrect and sometimes nonsensical results. The computer will blindly process any incorrect data and instructions'.

roles and capabilities. Sections 71, 146 and 147 of the *Evidence Act* 1995 (Cth) provides such acknowledgment. The presumption of accuracy of material produced by computing systems now allows into evidence the myriad of documents and business records generated from computer stored information. By removing the requirement for evidence as to the working accuracy of a particular device or process, the cost and time involved in litigation will be reduced. Further, the legislation supports the common law position thereby providing greater uniformity in this area of law.

Notwithstanding the benefits of such provisions, the life threatening consequences and significant economic impact of computer failure cannot be ignored. The courts and legal profession must necessarily become far more vigilant about the dangers inherent in technological devices, processes and machines. Better risk management and audit trails in documentation will assist in preventing computing faults. Business records, because of their nature, continuously undergo change. Audit trails may be placed in systems to track the use of the system both by authorised and unauthorised personnel.

The faults and errors which emanate from the use of computers and other electronic devices and programs substantiate the argument that it is in fact not correct to presume that each time a process or device which is ordinarily used to produce an outcome will produce the same result every time it is activated. Nor is it correct to assume that the information produced from such devices or processes will be accurate. It may indeed be argued that purely because of the nature of devices, machines and processes, it would be possible in every case by way of expert evidence, to raise doubt not only about their accuracy, but also the accuracy of the data processed or produced by the system. It would then be for the court, as pointed out by Wright J,[35] on the occasion in question, to determine whether sufficient evidence has been raised to cast doubt on the accuracy of such data.

Stamper warns that eliminating all error is impossible, but error prevention techniques can reduce the probability of error corruption in the data.[36] Evidence of proper maintenance (perhaps in the form of a log), the use of fault tolerant systems and programs, and the storage of documents and business records on CD Rom may go a long way towards eliminating any doubt which may be raised as to the accuracy of the information produced or processed by the device, machine or process on the occasion in question thus allowing the new provisions of the *Evidence Act* to provide the benefits intended.

[35] *Maynard* (1993) 70 A Crim R 133, 142.
[36] Stamper, op cit (fn 19) 97.