Electronic Documents as Evidence: an issue for all in-house counsel to consider

ALLISON STANFIELD
Founder, e.law Australia Pty Ltd, Australia

Background
The use of electronic information within companies is now the norm. We all use word processing tools to create documents and we all use email to correspond and exchange documents electronically. However, as in-house counsel, is there enough attention paid to the way in which the corporation's information is captured, stored and retrieved? If the firm becomes embroiled in litigation will it be a relatively straight forward process to access relevant documents and review, and can in-house counsel be sure that the evidence is admissible and can be authenticated?

The rules of evidence that have developed over many years at common law have now been encapsulated in the Civil Evidence Act 1995 (UK) and many other jurisdictions have done the same<sup>1</sup>. Documents are a unique form of evidence in that they can comprise both real and testamentary evidence. The contents of documents may be admitted into evidence pursuant to s.8 Civil Evidence Act 1995 (UK) and may be authenticated in a manner approved by the court.

Electronic documents contain additional information within them that are computer generated, such as meta data, which can be very useful in certain circumstances. The best example of meta data is the fields of information that accompany an email, such as the date sent, the author, the recipient/s, the subject and so on. These fields can be used as proof of certain things.

Electronic evidence is a relatively new phenomenon and is rapidly becoming the default form of documentary evidence. The sharp increase is explained by the prevalence of computers in day-to-day business and where documents are created in electronic format in the first instance. Email is now the leading form of communication and transactions commonly take place via electronic means and thus comprise electronic evidence.

A comparison of email and traditional paper correspondence demonstrates the differences between documentary evidence in paper format and documentary evidence in electronic format. This leads to the question: can electronic documents as evidence be authenticated in the same way as paper documents as evidence?

To answer this question we first need to look at the existing rules of evidence that deal with the admissibility and authentication of documentary evidence.

At common law, statements made in documents are considered hearsay and evidence must given by someone who made the document or otherwise had knowledge of the document. The Civil Evidence Act 1995 (UK), abolished the rule against hearsay for civil

---

<sup>1</sup> For example, see the Uniform Evidence Legislation in Australia; Evidence Act 1995 (Cth), Evidence Act 1995 (NSW), Evidence Act 2001 (Tas), Evidence Act 2008 (Vic)
proceedings, pursuant to s.1(1). If hearsay is intended to be adduced in civil proceedings, notice of such intention must be provided to the other party or parties in the matter.

Excluded from the rule against hearsay are public documents and documents created in the ordinary course of business. The definition of “document” in s.13 Civil Evidence Act 1995 (UK) provides a definition of document that is broad enough to cover documents in electronic format.

The business records exception has its genesis in the old bankers books rule\(^2\) where bank employees would enter records into large ledgers as part of their daily tasks. The rationale behind the rule was that employees were simply performing their job and had no reason to enter incorrect information. This rule has survived and is now equally applied to documents created in the ordinary course of business and stored on computer systems.

Therefore, business records may be admitted into evidence, and they are not considered hearsay, although the other side can object. However, this rule was developed based on paper documents. Whether this rule can continue to apply to documents that are created and stored electronically must be questioned. For in-house counsel, this issue is particularly relevant, because of the possibility that records may be accessed and changed, without the organisation’s knowledge or consent. Consequently, such records could be admitted without any requirement to show that the organisation’s system was secure or that the records were authentic.

Complicating this scene is the use of social networking sites such as Twitter, Facebook, MySpace, YouTube and Flickr, and where corporations store information in the cloud. Further, the use of smart phones to access information creates another set of evidence that needs to be considered in any discovery.

Although many corporations now have policies dealing with the use of social networking sites by employees, the fact remains that evidence may need to be retrieved from these social networking sites; the records are widely available and ubiquitous.

Information stored in the cloud poses a new set of problems for corporations, particularly if evidence needs to be obtained and used in proceedings. The cloud can also present advantages for the collection and presentation of evidence, since it may be easier to prove who accessed the records and when.

The fact these issues arise, when they did not exist in the world of paper means that the integrity of electronic documentary evidence must be examined. Wikileaks is perhaps the best example of the integrity of evidence being compromised. If Wikileaks can hack into government computers in order to leak highly sensitive data, how safe is data anywhere? If it is not really safe, how does one prove that it has not been tampered with and that a document is really what it purports to be?

**The differences between paper and electronic documents**

**Paper and electronic documents are very different**

Although documents do not need to be in paper\(^3\), the fact is that there are vast differences between paper and electronic documents. The most obvious difference is that the content and the medium are separate and distinct.

Electronic evidence requires a storage media and software to appropriately interpret and display the content. This can be clearly juxtaposed with paper, where the medium and content are tightly bound together.

\(^2\) Bankers’ Books Evidence Act 1879 (UK)

\(^3\) *R v Daye* [1908] 2 KB 333
A digital file does not exist independently from the media upon which it was recorded. At its lowest level, electronic evidence is in binary form (0s & 1s) and software is needed to interpret and display the information. Thus, electronic evidence requires a digital medium for storage (for example, a hard drive, a CDrom or USB memory stick) and appropriate software to interpret the electronic information. Both of these are required before the 'document', that is the content, can be reviewed. The document itself contains both the human-created content, as well as computer-generated metadata which is evidence in itself, as it can show the date upon which a document was created and certain other details about the document file.

With paper, the content cannot exist without the medium, whereas with electronic evidence, the content can reside on a number of disparate storage media. Further, the content requires a method by which to interpret the data. The rules of evidence that deal with documentary evidence were developed with paper media in mind, and those rules cannot be applied to electronic evidence in the same way.

Electronic evidence is capable of being stored in many different formats, upon many different media. Storage media can include personal computers, servers, mainframe computers, backup tapes, removable media and portable devices such as compact discs, digital versatile discs, blu-ray discs, USB flash drives, USB hard disc drives, CompactFlash cards, Digital Video Recorders, Mobile phones, SIM cards and Digital Audio Players.

The concept of a record created by one individual, stored in one place, is dissipating, as demonstrated by the use of cloud computing, where information is stored across different servers, perhaps even in different countries, and the use of cloud computing brings into play questions around the provenance of documentary evidence. The use of social networking sites means that documents can have more than one user; how is such evidence authenticated?

**Existing rules of evidence**

The rules of evidence governing documentary evidence were evolved over hundreds of years with respect to paper. Electronic documents and electronic communications have only become standard in the last 20 years. Yet, the laws of evidence that are being applied to electronic information are the rules that have been developed around the admissibility of paper.

This unique nature of electronic information means that a complete review of the evidentiary laws is required. For example, if electronic evidence needs to be authenticated, the methods are not as settled as with paper, such as with handwriting. The metadata associated with electronic files can be used as circumstantial evidence to prove a particular set of events. Emails in particular, can be difficult to prove given the lack of identification evidence.

The issue of authentication goes to whether the document is relevant and if it is not authentic then it will not be relevant. There is a need to prove that a document tendered is what it purports to be and before a document is admitted in evidence it is necessary to show that there is an evidentiary basis for finding that it is what it purports to be.

The business records exception to the hearsay rule is called into question because it is argued that no one person can give evidence as to the creation and content of electronic

---

evidence. Paul\(^5\) uses the example of a contract in a word processing format stored on a computer network within a company comprising 1,500 employees. Although a senior manager can attest to the content of the contract which may have been drafted several years\(^5\) previous, with the manager’s input, the manager cannot testify to the exact wording of any specific section of the contract without reference to it, nor can the manager testify to the systems used to store, backup up, audit and generally about the integrity of the document. How can the manager affirm that the document was not accessed by one of the other 1,500 employees? Unless the manager is also the IT administrator and that all of the required security elements are in place, the manager has no idea as to the integrity of the document.

For in-house counsel, this poses the question as to whether electronic record keeping systems are such that if information is being admitted into evidence, can the company attest to the fact that the electronic document in question has not been altered since its creation?

**Applicability of existing rules of evidence to electronic documents**

There has been a dearth of case law on the authenticity of electronic documents,\(^6\) and those that have considered electronic evidence have simply accepted the authenticity of documents without delving into the issue of whether the integrity of the evidence has been compromised, thereby calling into question authenticity.

Mason\(^7\) contends that a range of issues must be taken into account when considering whether to admit electronic information into evidence. In many cases, says Mason, oral and circumstantial evidence will be sufficient to provide for most documents in electronic format. Further, the medium upon which the electronic information is stored should be taken into account, since, for example, testing reliability for information stored on a mainframe computer will be different to that stored on a personal computer since the mainframe cannot be seized and moved.

In the USA, Paul\(^8\) recognises that the foundational requirement for authentication of electronic evidence has largely deteriorated into a ‘trivial showing’. Paul argues that due to the unique nature of electronic evidence, without demonstrating that the information was created and stored within a reliable system, the chain of custody necessary to show that a document is authentic is lost.

Similarly in Canada, Chasse\(^9\) argues that counsel and courts are simply ignoring the issues posed by electronic evidence with the consequence that electronic evidence is admitted without any form of effective authentication.

There is an argument that the rules surrounding authentication of evidence were formed around the need to authenticate paper documents and these rules no longer have application to electronic evidence where the evidence is no longer two dimensional. Rather, electronic evidence is comprised of a series of electromagnetic pulses which must be stored on a digital medium and which must be interpreted using specific software.


\(^8\) Ibid n3.

In the USA where the courts have had the opportunity to consider electronic evidence (or ‘electronically stored information’ (‘ESI’)), the application of the rules of evidence as they apply to electronic evidence has tended to be applied inconsistently and without adherence to a common standard.

As Paul\textsuperscript{10} notes:

‘.. the current system of foundations allows litigants to place into evidence almost anything they want so long as they can get a witness with some nexus to testify that a document is what it is claimed to be. They can employ a sort of legerdemain. If we are to be intellectually honest, there is almost no preliminary burden of providing digital information is authentic.’

In Canada, Chasse\textsuperscript{11} argues that the most serious failing of the business record provisions in the Canadian Evidence Acts are that:

1. They fail to inform adequately as to what evidence is needed for proof of the truth of business records sufficient to render them admissible in evidence; and
2. They allow court decisions to ride off in all directions because the tests they provide are undefined and too vague to command consistency in judicial interpretation.

The courts are allowed flexibility in applying the evidentiary rules, Chasse\textsuperscript{12} argues, and this leaves litigants and the business community uncertain as to what is required to prove business records as admissible and credible evidence.

When the business records exception to the rule against hearsay was developed, the courts recognised that companies need to keep complete and accurate records and at the time of making the record, there is little incentive to make inaccurate records. However, Chasse\textsuperscript{13} argues that in many situations now, incomplete and inaccurate records are necessary to maximise profits, or at least to minimise losses. Often it is more conducive to profit and to the avoidance of loss to destroy or "lose" embarrassing and damaging records than to comply with the demands for their production. Regulatory authorities have much greater powers to force production of records and disclosure of information, and these are being used more frequently.

The test of admissibility, Chasse\textsuperscript{14} argues, should be to judge not the record alone, but the record system it comes from and this can be accomplished by judicial interpretation that holds that evidence that satisfies the system integrity test of the electronic record provisions, satisfies the business record provisions, as well. Conversely, evidence that cannot satisfy the system integrity test should be held to be insufficient to satisfy the business record provisions.

Some commentators within Australia\textsuperscript{15} have recognised the necessity to ensure the integrity of a system to keep electronic evidence, however, this has not seen a transfer across to the rules of evidence. Certainly, commentators in other jurisdictions recognise the need for a system based integrity test, given that documentary evidence comprises paper on a diminishing basis. Rather, electronic evidence comprises an electromagnetic

\textsuperscript{10} Ibid n3.
\textsuperscript{11} Ibid n6.
\textsuperscript{12} Ibid.
\textsuperscript{13} Ibid.
\textsuperscript{14} Ibid.
medium which stores bits and bytes ("data"), software to interpret the data and the content itself. The old methods used to authenticate evidence which were developed on paper records can no longer applied.

It is arguable, then that the emphasis needs to shift to the integrity of the record-keeping system and the emphasis needs to be placed on the "system".

It is the author’s prediction that it is only a matter of time before a business record admitted under the statutory exceptions to the rule against hearsay, is called into question because its integrity has been compromised. If senior management cannot attest to the fact that records were secure from the risk of tampering, then there is the very real possibility that documents are accepted into evidence when they should first be proved.

To those who argue that this may impose unnecessarily stringent requirements into the evidentiary process, the response is that all that needs to be shown is that the company had in place a defensible, secure, auditable system in place that shows electronic records are reasonably secure from tampering.

If this move takes place, this will be particularly relevant for in-house counsel who will need to make sure that an organisation’s records are kept securely without risk of compromise, between the date of creation and the date of admission into evidence. This will mean that security and auditing of record keeping systems will be essential within every organisation.

**The record keeping system**

In order to show that an appropriate record keeping system is in place, in-house counsel should work closely with senior management and information technology staff members to put in place systems, processes and procedures that can enable verification of electronic information when required. If appropriate standards and procedures have been followed in the creation and maintenance of electronic evidence, the party endeavouring to prove the evidence will be in much better stead than if there are minimal standards and procedures.

When considering the weight afforded to copies of documents, the court may take into account the following factors:

- **Accuracy** – records were made and kept accurately;
- **Reliability & Integrity** – that the copies have been retained in a robust and secure environment;
- **Authenticity** – that the copies have not been tampered with in any way; and
- **Accessibility** – the copies can be accessible in years to come ie to ensure the records are accessible on current technologies.
- **An appropriate electronic document and records management system should be kept to capture electronic information and allow for quick and easy retrieval of information generally or for litigation purposes.**

Record keeping practices should be established, advised to all staff and followed. Adequate record keeping practices are the responsibility of each individual within the organisation whether they be senior management, administrative support staff or information technology professionals, so adequate training should be provided by the organisation.
Electronic records are not an information technology issue, rather they are a business issue with legal consequences. In-house counsel needs to work with senior management and IT to ensure the company's policies and procedures around the creation, storage and retrieval of electronic records are such that the integrity those records can not only be maintained, but verified.

Companies should ensure user access policies are well defined, implemented and regularly audited for unauthorised access.

If information is stored in the cloud make sure the contract with the cloud provider is negotiated in such a way that your company can have access to its data at any time and that data will be stored in a location that is approved.

If mobile technology is provided to staff, then PINs should be used to lock the devices to prevent unauthorised access. If staff need to access particularly sensitive material, then the company should utilise encryption technology for mobile devices, which makes it extremely difficult for the data to be accessed if the device falls into the wrong hands.

**Conclusion**

This paper rightly questions whether our existing rules of evidence adequately take into account the admissibility of electronic information, which has only been around for an extremely short time when compared to paper.

The rules of evidence should be changed to take into account the fact that we now live in a world where systems store our information and it is the integrity of those systems that need to be questioned, as these can no longer be compared to what we know about paper records.

***

**Allison Stanfield** founded e.law International in 1999 and has successfully run a number of high profile electronic trials and Royal Commissions. Her passion in this area has seen her write prolifically on the subject, having written two texts, many articles in published journals and now as a candidate for a PhD in the authentication of electronic evidence.

**e.law Australia Pty Ltd** provides niche legal technology services to the legal profession, corporations, the courts and government. Services include electronic data discovery, computer forensics and electronic trial services.