



ARMA International Educational Foundation

PROOF OF THE AUTHENTICITY OF A DOCUMENT IN ELECTRONIC FORMAT INTRODUCED AS EVIDENCE

Stephen Mason, Barrister

Visiting Research Fellow at the British Institute of International
and Comparative Law

Director of the Digital Evidence Research Programme:
<http://www.biicl.org/digitalevidence/>

October 2006
Project Underwritten by:

The ARMA International Educational Foundation
Endowment Fund

© 2006 ARMA International Educational Foundation
1609 Terrie Drive
Pittsburgh PA 15241 USA
www.armaedfoundation.org

Proof of the authenticity of a document in electronic format introduced as evidence

By Stephen Mason, Barrister

Introduction

The question of proving the authenticity of a document in analogue or digital (generically 'electronic') format is of great concern to information and records managers. This stems from core professional principles regarding the integrity of recorded information and techniques developed over time to be able to prove the authenticity of a record that is recorded on a tangible physical carrier, most likely to be paper. As a result, there has been a concern with the quality of the paper, together with procedures such as copying facsimile messages to bond paper, because the text printed on some types of paper used in facsimile transmissions tend to fade. Part of this effort is directed towards the objective of having an acceptable and authentic record that is admissible in a court. The same issues are of concern today, except the concerns of documents in electronic format include a mixture of the tangible and intangible.

This paper aims to discuss the legal requirements for introducing electronic documents into court as a form of evidence, mainly in the context of the jurisdiction of England and Wales, and some of the considerations that may be taken into account if a document in electronic format is challenged by either party to legal proceedings.

Terms

Two terms are widely used to describe documents in a format other than on paper: they may be described as electronic documents or digital documents. Either term may be correct, including documents in analogue format. These terms tend to be used interchangeably, and it is not the intention in this paper to deal with the differences in depth, but the meaning of these terms are considered briefly below. No critical analysis is offered, and the definitions are only provided to illustrate the nuances between the words in common use.

Analogue

The entry for analogue computer in Wikipedia provides a definition as follows:

‘An analog(ue) computer is a form of computer that uses electrical or mechanical phenomena to model the problem being solved by using one kind of physical quantity to represent another.’¹

The electronic version of the Oxford English Dictionary (second edition) provides a similar definition:

B. *adj. analogue* (U.S. analog) *computer*, a computer which operates with numbers represented by some physically measurable quantity, such as weight, length, voltage, etc. Also, *analogue device, machine, etc.* Hence *analogue computing*, computing by this process.’

Examples of analogue data include vinyl records, audio tape, photographic film, telephone calls made over the public switched telephone network, and human-readable paper documents. It is true to say that analogue systems are unlikely to generate evidence, although analogue data is more important from the point of view of the information obtained, such as the evidence of the photographic film and the photographs taken from the film, not necessarily from the camera that was used to take the film.

Digital

In the draft partial entry dated March 2003 to the electronic version of the Oxford English Dictionary (second edition), two definitions are offered, both of which help to explain the meaning of digital:

‘Relating to or operating with signals or information represented by discrete numeric values of a physical quantity such as voltage or magnetic polarization (commonly representing the digits 0 and 1); designating a signal or information of this kind. Opposed to *analogue*.’

‘Relating to or involving the capture, storage, or manipulation of images by digital means; (of an image) stored or represented digitally; (of a device) capturing or generating such images. Also in *Cinematogr.*: utilizing this technology in film or television production.’ⁱⁱ

The entry for digital in Wikipedia includes the following:

‘A digital system is one that uses discrete numbers, especially binary numbers, or non-numeric symbols such as letters or icons, for input, processing, transmission, storage, or display, rather than a continuous spectrum of values (an analog system).

....

The word digital is most commonly used in computing and electronics, especially where real-world information is converted to binary numeric form as in digital audio and digital photography. Such data-carrying signals carry either one of two electronic or optical pulses, logic 1 (pulse present) or 0 (pulse absent). The term is often meant by the prefix “e-”, as in e-mail and ebook, even though not all electronics systems are digital.’

Examples of digital data include anything that has been created or stored on a computer, or is made available by way of the internet, including CDs, DVDs, MP3s and digital broadcast radio.

Electronic

The term electronic may be considered to be a generative term, which encompasses all forms of data, whether in analogue or digital form; this meaning may certainly be inferred from the entry in the electronic version of the Oxford English Dictionary (second edition):

‘1. Of or pertaining to an electron or electrons.’

In comparison, the entry for the combination of the words ‘electronic document’ in Wikipedia provides a more meaningful definition within the context of documents stored in analogue or digital format:

‘Electronic document means any computer data (other than programs or system files) that are intended to be used in their computerized form, without being printed (although printing is usually possible).’ⁱⁱⁱ

In this paper, the term ‘electronic’ includes any information, whether it is in analogue or digital form that is carried by an electrical conductor.

Electronic documents

The range of documents that come within the term digital and electronic include, but are not limited to:

- Scanned image of a physical document.
- Files in native format, such as word processing documents in Microsoft Word format; spreadsheets in Lotus 1-2-3 format; presentations in Microsoft PowerPoint format, etc.
- Networked communications, such as e-mail and instant messages.
- Digitally generated images and digitally encoded audio and video.
- Records, indices, logs and files.
- Databases.^{iv}
- Records of transactions, in particular financial transactions.
- Pages from web sites.

This short list illustrates the vast array of digital evidence that is produced every day – perhaps every second of every day across the globe.

Testing physical documents in court

A range of evidential issues may arise in a legal context in relation to the introduction of a document, including the genuineness, authorship, attestation and other requirements that may affect the validity of the document. This paper will not consider such issues in depth, and the reader is directed to the standard legal texts on the topic for any given jurisdiction. In brief, the question of authentication relates to the question whether the document is what it purports to be. This is a matter of evidence, and an adjudicator will be required to determine the credibility or reliability of the evidence presented and tested before them. Generally, documents tend to be classified as public or private documents:

- **Public documents:** these comprise of published works that deal with matters of a public nature (such as histories, dictionaries), public documents (such as public registers), and records (for example, the records of certain courts, treaties, pardons). Usually, public documents are proved in court by the provision of a copy of the document, and the facts contained in the document apply against strangers as well as parties to the document.

- Private documents (such as a will or a bill of sale): the original document itself is required to be produced, and the facts contained in the document only apply against the parties named in the document (with the exception of England and Wales and Northern Ireland, where such documents may come within the provisions of the Contracts (Rights of Third Parties) Act 1999, for instance).

Whether a party is required to prove the authenticity of a document will depend on the rules of procedure. In England and Wales, by way of example, a party to civil litigation is deemed to admit the authenticity of a document disclosed to them, unless the party serves a notice that they wish the document to be proved at trial.^v Should a party require a document to be authenticated, then any presumptions that apply to the formation of a document will also be relevant (such as a presumption of the day a document is executed), and oral evidence will be required to test the validity of the document, such as:

- What the document actually comprises in physical terms.
- The source of the document. Factors in determining this will include whether there were any witnesses to the document being signed; if it has been signed by any of the parties; if there are any identifying features included in the document, such as name and address; if there is other evidence linking the document in question to help put it into context, such as related correspondence; the physical nature of the carrier, such as a letterhead; the existence of a post mark or other extrinsic evidence or testimony of any third party related to the transaction, including expert testimony.
- The integrity of the content. This will relate to the content of the document, and evidence of any tampering will be important.^{vi}

Lawyer's deal with forged or altered documents almost every day – from attempts by criminals to steal money, to claims that intellectual property really belongs to somebody else, backed up with forged evidence, or evidence that has been altered.^{vii} John D. Gregory has observed that the integrity of physical documents is 'often protected fairly causally',^{viii} yet the same could be said of documents held and created in electronic format.

One concern is whether the authenticity of electronic documents is subject to a more rigorous mechanism than would normally be associated with a document extant on physical media, although electronic documents also depend on physical media – the issue will be one of the degree of permanence. The two forms cannot be compared in this way, because the criteria by which a document in electronic format must be tested will differ, by its very nature, to that of a physical document. Both forms of document may have similar tests, such as testimony of creation and signature, for instance. However, the nature of the different type of documents will determine the most appropriate tests for authenticity.

For instance, the quality of documents in electronic format mean they have a number of features that present particular challenges that a paper carrier does not in the physical world:

- Data in electronic format is dependant on specific hardware and software to obtain access to it, and it is dependant on machines.
- Data in electronic format must be rendered into human-readable form through the mediation of a set of technologies. This means differences occur in how the same source object is displayed in different situations. A good example that is common to all users of the internet, is that a web site can look very different depending on when you view it and what browser you use, amongst other things. As a result, there can be no concept of a single, definitive representation of a particular source digital object.
- The technology changes rapidly, in the operating systems, application software and the hardware. As a result, electronic records may reach a point that they cannot be read, understood or used. Technical obsolescence is a major problem.
- Electronic documents are easy to manipulate: they can be copied, altered, updated or deleted with ease.
- The metadata can be fundamentally linked to a record in electronic format, included in the systems used to produce the record, within the electronic record, or linked from a separate system.
- The media upon which electronic documents are stored is generally considered to be fragile, although the same can be said of certain types of paper, especially if it is not manufactured to last very long – for instance, large quantities of paperback books published in the United Kingdom during the second half of the twentieth century were made with such poor quality paper that many have deteriorated over time. The media is inherently unstable, and unless the media is stored correctly, it can deteriorate quickly and without external signs of deterioration. Additionally, it is also at risk from accidental or deliberate damage and accidental or deliberate deletion.

It is inevitable that a document in electronic format invariably requires different mechanisms to test its authenticity, and to suggest the process may be more rigorous than for a physical document is to misunderstand the difference in complexity between the physical object and the electronic file.

Metadata

The term metadata refers to the data about data. It is a digest of the structure and subject matter of a resource. The metadata in relation to a piece of paper may be:

- Explicit from perusing the paper itself, such as the title of the document, the date, the name of the person that wrote it, who received it and where the document is located.
- Implicit, which includes such characteristics as the types of type used, such as bold, underline or italic; perhaps the document is located in a coloured file to denote a particular type of document; labels may also act as pointers to allow the

person using the document to deal with it in a particular manner, such as a confidential file, for instance.

Physical documents can be subject to intensive scrutiny, and the data contained on the document can be analysed in great detail. One example is document tav/149, which was adduced as evidence in the trial of Ivan Demjanjuk in the Special District Court of Jerusalem in 1986. The defendant was accused of being an accomplice to mass murder in the Treblinka camp, and, as a response to his alleged actions, was called by the prisoners of the camp Ivan Grozny, or Ivan the Terrible. The document in question appeared to be a service certificate in the guard forces in the service of the SS and the police in the eastern territory, situated in the Trawniki training centre, in the Lublin district of Poland. The certificate had the name of the defendant, together with further identifying particulars: date and place of birth, a photograph in SS uniform, which appeared to be his image, and the name of his father. The prosecution went to great lengths to prove this document was genuine and therefore authentic, especially in the light of the defence claim that it was a forgery by the KGB. Ivan Demjanjuk was found guilty of the charges. He was subsequently released in 1993 after an appeal hearing, which established the document was not what it purported to be, and another person was identified as the notorious guard at Treblinka.^{ix}

With electronic documents, the implicit data needs to be made explicit if it is to be used to help interpret the purpose of the electronic document. Such data can include, and be taken automatically from the originating application software, or supplied by the person that originally created the record.

Admissibility of documents in electronic format

In the main, the processes and procedures to be put in place to provide for the authenticity of a document in electronic format will vary between public documents, which are the responsibility of the relevant organ authorized by the legislature (such as the Keeper of Public Records in England and Wales), and documents created and distributed by the private sector, where there may be less of a need to follow stringent recommendations to preserve digital documents. However, some private organizations are required by regulatory authorities to meet stringent requirements, which in turn are enforced by substantial penalties.

The legal response in England and Wales to digital evidence has evolved since the early days of requiring evidence in electronic format, or taken from an electronic device, to be accompanied by a certificate that the machine is working. The developments of the English legal system with regard to the submission of electronic evidence into the courts in England and Wales will not be rehearsed in this paper. However, a brief overview of some basic terms will be of assistance.

Document

A document is defined in the Civil Evidence Act 1995 s13 as

‘anything in which information of any description is recorded, and ‘copy’, in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirect.’

The Civil Procedure Rules 1999 also provide a meaning of a document in Pt 31 r.4 as

‘... anything in which information of any description is recorded’ and a copy is, in relation to a document ‘... anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.’

These definitions illustrate the emphasis on the recording of the content, although a further statutory definition is provided in the Finance Act 1993 which specifically includes the use of the word ‘computer’:

“‘document’” includes a document of any kind whatsoever and, in particular, a record kept by means of a computer.’^x

Various other definitions are offered by statute, including the specification of the types of storage medium, defining documents by reference to lists and references to the use of documents in digital format.^{xi}

From the point of view of the common law, the meaning of a document has been restricted to its function as evidence, in particular to the process of disclosure. The concept of a document was the subject of *R v Daye*,^{xii} in which Darling J suggested that the meaning of a document should not be construed in a narrow sense

‘I think that it is perfectly plain that the sealed envelope itself might be a document ... I should myself say that any written thing capable of being evidence is properly described as a document and that it is immaterial on what the writing may be inscribed.’^{xiii}

In the modern context, audio tapes were accepted as a discoverable document in *Grant v Southwestern and Country Properties Ltd*,^{xiv} in which the meaning of a document was defined by its quality to convey information, and it did not matter what format the storage medium took.^{xv} The material may sometimes determine the admissibility of the evidence,^{xvi} but the definition is considered wide enough to bring any medium into its ambit without causing difficulties.^{xvii}

Writing

Writing is defined in Schedule 1 to the Interpretation Act 1978, and

‘includes typing, printing, lithography, photography and other modes of representing or reproducing words in visible form, and expressions referring to writing are construed accordingly.’

This definition emphasises the need for the writing to be in visible form, which appears to exclude information in electronic format, although microfilm and fiche are in writing, even though a machine is required to read the content recorded. This means that information in electronic format will only come within this definition if it comes within the method set out in the definition: ‘...and other modes of representing or reproducing words ...’^{xviii} In his conclusion of whether information in electronic format will amount to writing, Professor Reed suggested there were two possible approaches to this problem:

‘The distinction is not between information affixed to a carrier or not, but between informal speech and formally recorded information, in the same way that the content of a message was recorded by means of telegraph, although the problem

with this analysis is that there is no distinction between the use of the technology in a formal or informal capacity.

The second possibility is to suggest that the requirement of 'writing' is merely evidential in nature, although the courts continue to maintain the position that tendering oral evidence cannot rectify the lack of formality.^{'xix}

It is useful to note the range of functions that writing performs in relation to a physical carrier, as considered in the UNCITRAL Model Law on Electronic Commerce:^{xx}

'... the following non-exhaustive list indicates reasons why national laws require the use of 'writings': (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) to help the parties be aware of the consequences of their entering into a contract; (3) to provide that a document would be legible by all; (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (5) to allow for the reproduction of a document so that each party would hold a copy of the same data; (6) to allow for the authentication of data by means of a signature; (7) to provide that a document would be in a form acceptable to public authorities and courts; (8) to finalize the intent of the author of the 'writing' and provide a record of that intent; (9) to allow for the easy storage of data in a tangible form; (10) to facilitate control and sub-sequent audit for accounting, tax or regulatory purposes; and (11) to bring legal rights and obligations into existence in those cases where a 'writing' was required for validity purposes.'^{xxi}

Record

The need to define a record is of relatively recent origin. A definition is provided in s13 of the Civil Evidence Act 1995 as 'anything in which information of any description is recorded' and this definition is also adopted in CPR Pt 31, r. 4:

'Copy' in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.'

In respect to the use of 'record' in statute, the majority of provisions bring information in electronic format within the ambit of a record, although a number of statutes may make assumptions that records are retained in hard copy. The case law illustrates that the meaning of 'record' is discussed in relation to the admissibility of a body of evidence and the purpose for which the record has been made.^{xxii}

Instrument

Of the references Professor Reed found when researching his book where the word 'instrument' was used in a statute, only one statute, s8(1) of the Forgery and Counterfeiting Act 1981, specifically referred to digital information, whilst other definitions refer to 'document' that does not necessarily exclude digital information.^{xxiii} The meaning given to the word 'instrument' was discussed in *R v Riley*^{xxiv} where the prisoner sent a telegram to a bookmaker after he knew the winner of the Newcastle Handicap run at 2.45pm on 27 June 1895 was named Lord of Dale. He contrived to make it appear that the telegram was sent from a sub-post office, which would mean the

telegram would not arrive with the bookmaker until some time after the race was run. However, he actually sent the telegram from the head office after the news arrived in the office that Lord of Dale had won the race. The court held that a telegram amounted to an instrument for the purposes of s38 of the Forgery Act 1861. In his judgment, Hawkins J suggested the word should be interpreted according to its ordinary meaning, and quoted a number of dictionary meanings before concluding that they covered an ‘infinite variety of meanings.’^{xxv} In his judgment, Willis J concurred, and went on to offer the following comment:

‘I cannot see anything in the nature of such a section which should make it necessary or desirable to restrict the application of the word ‘instrument’ to writings of a formal character, and I think it is meant to include writings of every description if false and known to be false by the person who makes use of them for the purpose indicated.’^{xxvi}

Lord Russell of Killowen CJ and Vaughan Williams J had reservations about the meaning of the word in the context of the Act, although Vaughan Williams J accepted the word had been used in a narrow, restrictive meaning that referred to the formation of a legal document, to the wider meaning adopted by Hawkins and Willis JJ. Professor Reed’s comment on this case:

‘However, it must be recognised that in 1896 a non-written document would be abnormal, and the case cannot be considered as a very strong authority for the proposition that an electronic record cannot be an instrument’^{xxvii}

must be correct, although there is a good reason to suggest that there is a reason why this case may appear to be helpful in the context of electronic data. This is relates to the method by which the telegram came into being to begin with. As discussed above, the sending party may write down the message on a form or dictate it to an operator. The operator would then send a series of electronic pulses to the receiving operator, who in turn would interpret the code and write the text down by hand. This carrier forms the ‘document’ or ‘instrument’. No consideration in this case was given to the transmission of the original text to the receiving operator, yet the telegram received by the bookmaker was considered to be a document. It could be argued that information in electronic format is identical in concept to the pulses passed over a telegraph wire, with the exception that technology can now store the message in electronic format, which was not possible with the telegraph.

European Union

The European Union, in the context of electronic signatures, has provided that such signatures cannot be denied legal effectiveness solely on the grounds that they are in electronic format. Under the provisions of article 5 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,^{xxviii} provision has been made to ensure that advanced electronic signatures are admissible as evidence in legal proceedings, and other forms of electronic signature are also admissible:

‘Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based

on a qualified certificate and which are created by a secure-signature-creation device:

- (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
- (b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.’

There was no requirement to provide for the general admissibility of electronic signatures under both US and English law, as demonstrated in the United States case of *Wilkins v Iowa Insurance Commissioner, Wilkins v Allstate Insurance*^{xxix} and in England by the Industrial Tribunal case of *Hall v Cognos Limited*.^{xxx} However, Parliament subsequently passed the Electronic Communications Act 2000, and to correct a failure to incorporate the entire provisions of the EU Directive into the Act, followed this with the Electronic Signatures Regulations (Statutory Instrument 2002 No 318) two years later.

Authentication of electronic documents in dispute

Where the authenticity of a document is the subject of a challenge in legal proceedings, a range of evidence may be required, covering some or all of the technical attributes associated with the preservation of electronic documents. In preparing and presenting evidence of the authenticity of an electronic document, reference will undoubtedly be made to standards, both national and international. In addition, authoritative papers, such as those prepared by the National Archives in the United Kingdom (Generic requirements for sustaining electronic information over time), and the National Archives of Australia (Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records) will also be of help in establishing and testing the authenticity of the document in question. Finally, the services of a digital forensic expert may also be necessary, depending on the facts in issue.

The evidence to defend, and in turn, to test, the authenticity of a document in electronic format will be determined by the precise nature of the document in question: whether it is in analogue or digital in form, for instance; by way of example, whether it is an image of a photograph, which in turn could be in digital format or a negative on a film.

The type of evidence available to a court to determine the authenticity of document in electronic format, will comprise a mix of technical attributes and organizational matters. However, the comments and underlying assumptions made by authors of the technical literature appear to assume that the nature of the evidence builds to form a cohesive

whole. For instance, it is stated by the author of ‘Generic requirements for sustaining electronic information over time: 1 Defining the characteristics for authentic records’^{xxxii} that authenticity can only exist if the three characteristics set out in BS ISO 15489-1:2001 ‘Information and documentation. Records management. General - reliability, integrity and usability’, are also present. The suggestion is that:

‘As such authenticity is an implicit value derived or presumed from the presence of the explicit elements that characterise the other three characteristics. A presumption of authenticity is an inference that is drawn from known facts about the manner in which a record has been created, handled, and maintained.’

This is an attractively sound proposition, but although the mass of evidence may appear to have a cumulative effect, the failure in any single part of a technical or organizational characteristic will serve to undermine the totality of the evidence. According to the author of ‘Admissibility Of Electronically Filed Federal Records As Evidence’,^{xxxiii} in 1990, cross-examination in relation to the integrity of computer stored or generated files include questioning:

- the source of the input data or information and the process for transcribing it to machine readable form;
- the computer programs that create, edit and update the files;
- the computer programs that produce the output or stored files; and
- the reliability of the hardware and vendor-supplied ‘off-the-shelf’ software that systematically manages the internal processes of the computer.

In this respect, the lawyer whose duty it is to test the evidence is not interested in the gradual build-up of the various layers of technical and organizational characteristics that form the basis for the authenticity of a document in electronic format. They are interested in exposing weaknesses, and if it can be demonstrated that a sufficient number of weaknesses exist, the totality of the cross-examination may mean the party submitting the document has failed the evidential burden of convincing the adjudicator to accept the evidence.

However, the guidance issued by various public record offices across the world in relation to the authenticity of electronic records remains sound. Procedures, process and technical measures such as audit logs, system security and the use of digital signatures are all highly relevant in providing for the authenticity of documents in electronic format. The development and provision of standards and guidelines is merely one part of the whole. The most significant issue in relation to this matter is how such standards or guidelines are actually implemented. The gap between what is stated in the standard or guideline, and what actually occurs in reality, will be a central focus of cross-examination in a court.

Issues to be taken into account for the authenticity of electronic documents

The range of issues that may need to be covered when introducing electronic data into court will depend on local procedural and evidential rules. Of interest is a recent decision

in the United States of America. The case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company, Inc. v Vee Vinhnee*^{xxxiii} deals with the evidentiary foundation for introducing electronic business records. In this case, American Express claimed Vinhnee failed to pay credit card debts, and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in electronic format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Klein J, pointed out, at 444 [14] that:

‘... the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.’

In essence, the learned judge made the pertinent point that the issue is ‘Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be.’^{xxxiv} The learned judge continued to explain the issues involved in this process, at 445 [16]:

‘The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity’s policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

There is little mystery to this. All of these questions are recognizable as analogous to similar questions that may be asked regarding paper files: policy and procedure for access and for making corrections, as well as the risk of tampering. But the increasing complexity of ever-developing computer technology necessitates more precise focus.’

Judge Klein reached the conclusion that early attempts at establishing a foundation for electronic evidence were too cursory, whilst also accepting that judicial notice is commonly taken of the validity of the theory underlying the use of computers and the validity of the data generated generally. The learned judge then set out the tests described by Professor Imwinkelried in respect to considering electronic records as a form of scientific evidence.^{xxxv}

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.

6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms the witness explains the meaning of the symbols or terms for the trier of fact.'

The learned judge amplified the fourth step as follows, at 446[16]:

'The "built-in safeguards to ensure accuracy and identify errors" in the fourth step subsume details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records.'

The members of the court then proceeded to evaluate the exhibits submitted by American Express using the tests set out by Professor Imwinkelried. It was made clear that the evidence of the custodian of the records at American Express was far too vague to be accepted. The following problems were identified:

- Generally, the evidence was vague and unpersuasive.
- The custodian did not have the requisite knowledge to provide the evidence.
- The person providing evidence on behalf of American Express merely asserted that he was an employee of American Express and was personally familiar with the systems, both hardware and software. He failed to inform the court of his job title or of his relevant experience and training that would provide an element of authority to his evidence.
- American Express failed to provide information about its computer policy and system control procedures, control of access to the relevant databases, control of access to the applicable programs, how changes to the data recorded or logged, what backup practices were in place, and whether there were any audit procedures used to provide assurance of the continuing integrity of the records.

Although it will not be relevant or necessary to provide such an in-depth analysis of electronic records in every case brought before a court, nevertheless the comments made by Klein J help to illustrate the nature of the evidence that should be gathered, if it is necessary to adduce such evidence.

The following section sets out, in general terms, some of the issues that records managers should give some thought to in respect to electronic documents. A great deal of more detailed information is available from the free guidance offered by various national archive offices, and although the guidance mostly refers to the requirements to retain and archive public records, nevertheless the literature can help commercial organizations more fully understand the issues relating to the management of digital documents. It is

not intended to repeat the work and guidance already freely available, details of which are set out in the bibliography section.

It should be noted that the comments offered below are general in nature, and do not take into account the differences adopted between records managers and archivists with respect to appraisal or scheduling.

Technical

Method of preservation

Several methods are used to preserve electronic data. Risks attach to whichever method is used, and it is important to ensure that whatever method is employed, it can be defended should the electronic document be the subject of a legal challenge as to its authenticity.

- Technology preservation. This is the creation of a methodology to conserve the environment in which the data files are set. This includes the software and hardware to enable a user to obtain access to and read the data. It is probable that this option is not a viable alternative, given the costs involved in supporting and maintaining obsolete hardware and software. An added factor to take into account is the deterioration of the media itself.^{xxxvi}
- Technology emulation. This can take different forms. In essence, this is a method to run the original data and software on a new or current platform, or emulating a virtual environment. This can be achieved by running software on the new platform that emulates the original platform. Detailed information about the original environment must be stored alongside the digital data itself. Such methods are difficult to develop, and the authenticity of the data will depend on the links between the emulator to the emulated system.
- This method relates to the format in which the data is encoded. The data is copied to the latest form of storage media. Data is converted from one file format (which can no longer be read using the current software) to another format (which is readable with current software). Where the document has been part of a software migration, evidence will be required setting out why migration took place; the methods used to effect the migration; how the quality of the document was validated after migration, and records will be required setting out the names of the people undertaking the exercise, what they did and when they did it.
- Data Refreshing. This is where data is copied from one set or copy of the digital media to another of the same kind. It can also involve the copying of the data between media of the same type, or to a different kind of media.

This discussion does not consider the issues relating to the format by which documents can be, or ought to be, retained. Two cases that have occurred in the United States of America serve to highlight how concerns relating to the preservation of data are viewed. In the case of *Armstrong v Executive Office of the President, Office of Administration*,^{xxxvii} researchers and non-profit organizations challenged the proposed destruction of federal records. The Executive Office of the President, the Office of Administration, the National Security Council, the White House Communications Agency, and Trudy Peterson, Acting Archivist of the United States, intended to require

all employees to print out electronic communications on to paper in an attempt to discharge their obligations under the provisions of the Federal Records Act. The members of the United States Court of Appeals, District of Columbia Circuit, rejected this solution, because the hard copy printed version ‘may omit fundamental pieces of information which are an integral part of the original electronic records, such as the identity of the sender and/or recipient and the time of receipt’ in the words of Mikva, CJ at 1277, although the judgment dealt with the technical issues in slightly more detail than these initial comments by Mikva, CJ.

By comparison, in the case of *Public Citizen v Carlin*,^{xxxviii} the plaintiffs, representing historians, researchers, journalists, and libraries, challenged the General Records Schedule 20 dated 1995, and issued by the federal Archivist that governed the disposal of electronic documents created by federal agencies. Advice was given in this Schedule that permitted agencies to retain records in hard format, rather than in electronic format. It was this part of the Schedule that was in issue. The United States Court of Appeals, District of Columbia Circuit rejected the notion that all records created in electronic format had to be archived in electronic format.

Essential technical characteristics

Identity

The identity of the document will need to be established, such as the name of the purported author, the date it was created, the place of origin and the subject matter. It can be argued that this information forms part of the reliability of the document, meaning if it can be identified correctly, there is a degree of certainty about the document that could be relied upon.

Integrity

Integrity, as discussed in ‘Generic requirements for sustaining electronic information over time: 1 Defining the characteristics for authentic records’^{xxxix} is considered to refer to the ‘wholeness and soundness’ of the document. This in turn is related to whether the document can be considered to be complete and uncorrupted ‘... in all its essential respects during the course of its existence,’ whilst BS ISO 15489 provides that integrity refers to the record being complete and unaltered. While these definitions of ‘integrity’ might relate to the ability to verify that the content of a document has not been changed since it was written, finished and adopted by the author (if the author is known, or remains anonymous for good reasons), it might be necessary to consider other matters, including, but not limited to:

- Whether a time stamp was used, and if so, whether it can be considered to be accurate, and if in doubt, what standards were observed with the particular type of time stamp used.
- Whether it is a partially written document.
- Whether the test for integrity of the document should only apply to the original version (whatever that may be), or whether any tracking regarding the document’s subsequent circulation is necessary. Following from this, the integrity of the circulation metadata may be required.

- Whether the metadata can be accepted as reliable and meaningful.

The concept of integrity will be closely related to the organization's control over the preservation of a document, and this is discussed in more detail below. Underlying the integrity of a document will be the use of digital signatures to provide evidence of verification that the document has not been altered.

Usability

The term usability is meant to cover the practical issues relating to retrieving, presenting and interpreting the data correctly.

Attributes of storage

The attributes of long term storage of documents in electronic format need to be addressed. A range of issues arise from this perspective, mainly, but not exclusively around technical obsolescence, which affects:

- The media upon which data is stored.
- The application software used to create, process and display data is replaced frequently, and some types of system software and middleware that are required by an application in order to work, also change. This issue will affect older electronic documents that were generated using software and machines that no longer exist. To be read, the text will require the use of different tools. The next question will be whether the application of a different tool affects an electronic document in some way.
- The architecture of hardware changes, because machines are replaced, which means some types of software will no longer be available, supported or maintained. In this respect, digital signature systems may be a problem. The digital signature software may still be available, but the digital signature might have been applied using a version of the software compatible with Windows 98, but not Windows XP, or the signature software tool may have been overtaken by something better, so the question then has to be asked whether the digital signature ought to be migrated, for instance, by using a further digital signature to provide for the integrity of the version that is migrated.^{x1}

Organizational characteristics

Procedural controls provide circumstantial evidence of the integrity of a document in electronic format. Where policies and procedures are followed, a degree of trust is created that acts to reinforce the probability that a document can be trusted. However, the assumption of integrity cannot be sustained where the procedures are tested in a court and found wanting by the adjudicator. This is why some or all of the following are relevant:

- The controls in place to prevent the modification or editing of the record.
- Evidence of the controls to support the document is authentic by the production of credible metadata, audit trails and relevant reports.

- The procedures in place to assess and maintain the authenticity of the document over the period of time it has been preserved.
- Evidence is available to demonstrate policies were properly created, and that procedures were subsequently adopted and followed to ensure the policies were correctly implemented.

Proving authenticity: evidential foundations in proving an electronic document in court

The tests proffered by Professor Imwinkelried offer a useful starting point for the introduction of evidence in electronic format, particularly in circumstances where a party is required to lay the evidential foundations of the evidence. As the Vinhnee case illustrates, a number of steps may be required if the authenticity of a document in electronic format is in question.

1. A decision may be required whether an expert witness is required. Such witnesses are more frequently required in giving evidence in criminal trials, but it may be necessary to seek the professional services of an expert witness if the party put to proof of a document in electronic format does not have the in-house capability to provide a witness with sufficient knowledge to provide the underlying technical foundation.
2. The witness will be required to demonstrate their expertise in the normal way, and to cover such issues as their job title, relevant experience, training and qualifications.
3. Evidence covering the technical and organizational issues outlined above will be required, including any policy and system control procedures, control of access to the relevant databases, control of access to the applicable programs, how changes to the data were recorded or logged, what backup practices were in place, and whether there were any audit procedures used to provide assurance of the continuing integrity of the records.
4. A range of associated issues may have to be covered, including the following:
 - a. The form of the record: whether it is provided to the court in native format (if so, whether the document has been altered); whether it is a scanned paper document (if so, it may be necessary to demonstrate that the process of scanning was such that the scanned document is a true replica of the original document, and there was no possibility of the document having been manipulated or altered between being received as an original document on paper and being added to the database in electronic format); whether it has been re-published in electronic format, such as PDF, and whether the document in question has been migrated between formats (evidentiary foundations will be required to demonstrate the efficacy of the process and what, if any, data was lost in the process).
 - b. The process of authentication may require evidence relating to the machine that was used to retrieve the document (was the machine the original as used 20 years ago, or is it a modern machine, and if a modern

machine, was any data associated with the document lost in the process when retrieving the document); the type of operating and application software used when the document was first created, and whether subsequent changes to both the operating and application software have altered the underlying integrity of the document in any way; whether the storage medium, and any migration between storage media has altered the document; whether the method of retrieval has affected the document; whether it is possible to detect alterations to the document.

In essence, the characteristics of authentication comprise reliability (there is evidence that records are created and captured as part of the legitimate business process, and they are subject to a corporate management process), integrity (the document is protected from unauthorized alteration) and usability (the document is capable of being retrieved, presented and interpreted correctly). These characteristics, taken together, lay the foundations for the authenticity of a document in electronic format. However, it must be emphasized that the rigour of the process will depend on the nature of the document. Admitting a statement of account as part of a business process may well be an easier exercise than, for instance, a scanned copy of a will.

Practical advice

Although documents in digital format present a particular set of unique problems for their long-term conservation, nevertheless, a number of very helpful initiatives have already provided a substantial amount of information and advice on this topic, as indicated in the biography. From the point of view of the records manager, the most difficult question remains: how to preserve digital records. Unfortunately, the answer to this question is somewhat of a moving target, because the nature of the technology determines the answer to a certain extent.

The length of time a document needs to be retained is a useful starting point from which to begin to plan for the preservation of digital records.^{xli} The Digital Preservation Coalition provide the following guidance and definitions:

‘Short-term preservation - Access to digital materials either for a defined period of time while use is predicted but which does not extend beyond the foreseeable future and/or until it becomes inaccessible because of changes in technology.

Medium-term preservation - Continued access to digital materials beyond changes in technology for a defined period of time but not indefinitely.

Long-term preservation - Continued access to digital materials, or at least to the information contained in them, indefinitely.’^{xlii}

Short term preservation

Short-term preservation should not pose a great practical problem. For the purpose of the legal context, the definition of short term is the longest period that the vast bulk of documents should be retained as determined by national legislation. In practice, this means most documents will need to be retained for up to seven years. Examples include the requirement to retain records of annual accounts, tax receipts and a wide range of documents created daily by all organizations that are necessary to continue the

administration of the business, whether in the public or private sector. In dealing with such digital documents, it is feasible to retain them in storage in native format until they can be deleted. Data that only needs to be retained for a short term will probably not need to be migrated. The main issue when dealing with documents over the short term is to demonstrate that the appropriate controls are in place to prevent unauthorized access, maintain the integrity of the data, and refreshing the media upon which the data is stored.

Medium term preservation

Medium term preservation can pose a more significant problem. For the purpose of the legal context, the definition of medium term is up to twenty years, by which time the vast majority of documents will have ended their statutory shelf life, although for practical purposes, the problems accompanying medium term and long term preservation may be considered identical. Examples from the United Kingdom include documents relating to company shares (to be retained for 20 years), contracts under seal (legal action can begin up to 12 years after performance) and documents relating to product liability. It may be possible to retain medium term records in native format, but taking into account the rapid changes to both application software and operating systems during the past twenty years, it is highly probable that the original documents cannot be stored effectively, unless they are migrated effectively to more up-to-date formats. The changes in technology will determine how documents that fall into this category are dealt with.

Long term preservation

Long-term preservation poses the greatest challenge to the preservation of digital documents. Of necessity, documents will have to be migrated from one format to another, and it might be that the document will need to be migrated several times during the course of its life span. For these reasons, a range of best practices have already been considered by a number of well-respected state organizations, in particular state archivists responsible for the preservation of state papers.

Arguably, no single set of coherent guidelines can be offered to records managers or archivists to enable them to fulfil the twin requirements of long term preservation and the legal admissibility of a document in electronic format, although the University of Pittsburgh 'Functional Requirements for Evidence in Recordkeeping Project' did attempt such an exercise. Three main components were identified: the functional requirements for recordkeeping for a number of purposes (legal, medical, business); a generic specification of the attributes relating to evidential properties in respect of accountable recordkeeping systems, and finally, the requirements that relate to the record itself.^{xliii} It is impossible to predict what future challenges might be brought against any particular document in digital format. To know how any single digital document will be challenged at a point in time in the future, is to have foresight of the particular problem that will be the subject of proof. All the archivist or records manager can do is follow the best advice available at the time that preservation is necessary. The preservation process ought, at the very least, to follow the accepted standards as developed at the time the digital records are preserved.

Policies and procedures

Perfection is impossible, and preserving digital records is no different. To preserve a document for the specific purpose of adducing it into evidence requires a foresight that we do not have. For instance, a number of questions present themselves, none of which will be known at the time the document was preserved:

Which document will be required in the future?

What particular problem will there be in relation to this particular document?

Will the procedures that were used to control access to the document be called into question?

Will the way in which the document was handled be cross examined?

Will the method used to migrate the document be tested?

Will the metadata be of any relevance? If so, which part of the metadata?

The practical point to reinforce, is that the deliberate preservation of digital data can only be undertaken using the best practice at the time of preservation, and it is for an adjudicator to determine what the best practice was or ought to have been. The essential point to grasp is this: document everything that is done to provide for the preservation of data. Even if the actual process might not be accepted in the future, it is probable, providing the process has been scrupulously well documented, that it will more readily withstand scrutiny in a court.

The 'Heiner Affair' in Queensland, Australia, highlights the problems that a state archivist may have when political pressure is brought to bear on the decision whether to retain certain documents. In 1989, Noel Heiner, a retired stipendiary magistrate, was requested to chair an inquiry into the management of the John Oxley Youth Centre in Wacol, Queensland. The papers produced by Mr Heiner during the course of his enquiry were subsequently handed over to the Queensland Department of Family Services and Aboriginal and Islander Affairs, and they were later sealed. These materials were then passed on to the Cabinet secretariat, and they were, in turn, passed to Ms Lee McGregor, the State Archivist. On 23 February 1990, an official from the Cabinet secretariat, Stuart Tait, requested Ms McGregor to destroy the documents. Approval was given, apparently within hours, and they were destroyed on 23 March 1990. The manager of the youth Centre, Peter Coyne, requested sight of the documents both during and after the inquiry ended, and was refused. The issues surrounding this inquiry became the topic of a great deal of public scrutiny, and a number of questions were raised, including:

- The nature of the discretion given to a State Archivist to dispose of official records.
- Whether the State Archivist is required to carry out instructions for the disposal of documents issued by a government.
- Whether records should be destroyed if they may be required as evidence.^{xliv}

In this particular case, the guidance, despite being extensively discussed by archivists, appears to have been minimal in Queensland. There may be a case to challenge the

decision-making process as to whether to retain a document, but the key to preventing a successful challenge must rest in the policies that are in place, how they are put into effect, and whether they can be considered to be appropriate for the nature of the documents that are stored.

An outline of the considerations to take into account include the following:

A focus on the document

- Determining the originality of the data to be preserved.
- The retention and preservation of the data that makes it a complete record.

A focus on the technical process

- Providing for the reliability of the process of the creation, capturing and handling of the data.
- Providing for the integrity of the data, both in respect of the technology used and the processes that control the data.
- Aiming to ensure the data can be retrieved and interpreted correctly.

A focus on the organizational process

- Ensuring the policies and procedures to handle the data are properly documented, and there is evidence to demonstrate that the policies are followed.

By following the guidance offered by national and international organizations on this topic, the records manager or archivist can offer evidence that goes to show that they will have undertaken their duties to the best standards available at the time the data is preserved. We cannot know what challenges will be made against evidence in electronic form in the future. At best, records managers and archivists should follow accepted standards and practice. It will be for lawyers to argue in the future, should the admissibility or authenticity of the electronic evidence be in issue, that the electronic data in question was secured by adhering to the best practice that was generally accepted at the time it was preserved.

However, from the point of view of a lawyer, it is necessary to ensure that criteria is agreed and documented when making decisions relating to documents in electronic format, and appraisal methodologies for approaching electronic records should be developed and maintained. Failure to have any criteria in place, and failure to implement decisions in relation to the criteria, will undermine the authenticity of the evidence. Where the evidence is in dispute, these factors will be the subject of extensive cross-examination. Where it can be demonstrated that there was no, or hardly any criteria, and the documentation relating to the criteria either does not exist or is poorly documented, such a lacunae will completely undermine the value of the evidence, and may well prevent it from being adduced into the proceedings, as in the *Vinhnee* case.

Regardless of whether information and records managers turn to national and international standards to implement relevant policies for the retention and long-term archival of data in electronic format, the central issue in ensuring the document can be adduced into evidence is to ensure there is no difference between the claims that a policy

existed and the documents relating to the policy were properly drawn up, and any failure to abide by the policy or standards in practice. If there is a difference between the rhetoric and the reality, the opposing lawyers will mercilessly expose the gap, if you own lawyers do not do it for you before the action begins.

© Stephen Mason, 2006

Stephen Mason is a barrister [<http://www.stpaulschambers.com>] with an interest in electronic signatures, authentication, security, electronic evidence, e-mail and internet use, and interception and monitoring of communications. He is a member of the IT Panel of the General Council of the Bar of England and Wales, and presently the Director of the Digital Evidence Research Programme at the British Institute of International and Comparative Law [<http://www.biicl.org/digitalevidence>], and an Associate Senior Research Fellow at the Institute of Advanced Legal Studies.

As far as he is aware, he was the first lawyer to write an e-book in 1999 on the Y2K issue, and he was also the first barrister to write a set of e-commerce precedents for lawyers on behalf of the Butterworths Tolley *Electronic Business Law* web site in 2000. Stephen drafted the evidence part of the ISEB syllabus for the Certificate in IT Law Foundation, established in 2005.

Stephen is the author of *Electronic Signatures in Law* (LexisNexis Butterworths, 2003) and *E-Mail, Networks and the Internet: A Concise Guide to Compliance with the Law* (xpl publishing, 6th edn, 2006), and the general editor of the *Digital Evidence Journal, incorporating the e-Signature Law Journal* [<http://www.digitalevidencejournal.org>].

He is also the electronic and digital signatures editor and author of Chapter VI 'Electronic and Digital Signatures' for the practitioner loose-leaf textbook by M-T. Michéle Rennie *International Computer and Internet Contracts and Law* (Sweet & Maxwell).

stephenmason@stephenmason.co.uk

Acknowledgments

I thank Nicholas Bohm, solicitor and e-commerce consultant to Fox Williams; Philip Lord and Alison MacDonald from the Digital Archiving Consultancy; Andrew Sheldon of Evidence Talks; Peter Sommer, Visiting Fellow, IS Integrity Group, London School of Economics and Dave Walker, senior security consultant, Sun Microsystems UK Limited for helping to formulate the first outline of the response to the question posed by this paper, and subsequently for their company on 14 March 2006 at the British Institute of International and Comparative Law, when we discussed the matter in more detail.

Further thanks also to Preston W. Shimer, FAI, Foundation Administrator, ARMA International Educational Foundation, Nicholas Bohm, Richard J. Cox, Professor, Archival Studies, Doctoral Studies School of Information Sciences, University of Pittsburgh, and Adrian Brown, Head of Digital Preservation at The National Archives, for their extremely useful comments on various versions of this paper. Also to Tom Worthington for providing me with a number of additional Australian references relating to standards.

Bibliography

This bibliography is not meant to be exhaustive. The reader is referred to the extensive cross referencing that occurs between web sites, together with the references provided in some of the texts set out below for further information.

Ariadne, available in electronic format at <http://www.ariadne.ac.uk/>

Authenticity in a Digital Environment (Council of Library and Information Resources, May 2000) available in electronic format at <http://www.clir.org/pubs/reports/pub92/contents.html#introduction>

Australia, National Archives of

Archiving Web Resources: Guidelines for Keeping Records of Web0based Activity in the Commonwealth Government (March 2001)

Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records (Exposure Draft May 2004)

Functional Specifications for Electronic Records Management Systems Software (Exposure Draft February 2006)

Guidelines for Implementing the Functional Specifications for Electronic Records Management Systems Software (Exposure Draft February 2006)

Helen Heslop, Simon Davis and Andrew Wilson 'An Approach to the Preservation of Digital Records' (National Archives of Australia, December 2002)

Australian Standard for Records Management – AS ISO 15489 available in electronic format at <http://www.standards.org.au/>

Neil Beagrie and Maggie Jones, 'Preservation Management of Digital Materials: A Handbook' (Digital Preservation Coalition) available in electronic format at <http://www.dpconline.org/graphics/handbook/>

David Bearman and Ken Sochats, 'Metadata Requirements for Evidence', available in electronic format at <http://www.archimuse.com/papers/nhprc/BACartic.html>

Filip Boudrez, and Sofie Van den Eynde, 'DAVID Archiving e-mail' (Leuven, August 2002, Version 1.0)

Canada, 'Uniform Electronic Evidence Act Consultation Paper' (March, 1997), available in electronic format at <http://www.ulcc.ca/en/poam2/index.cfm?sec=1997&sub=1997hka>

Cedars (Cedars began in April 1998 and ended in March 2002; its broad objective was to explore digital preservation issues), available in electronic format at <http://www.leeds.ac.uk/cedars/index.html>

Council on Library and Information Resources 'The Evidence in Hand: Report of the Task Force on the Artifact in Library Collections' (November 2001) available in electronic format at <http://www.clir.org/PUBS/reports/pub103/contents.html>

Michael Day

'Metadata for digital preservation: an update', available in electronic format at <http://www.ariadne.ac.uk/issue22/metadata/>

Digital Curation Manual Instalment on "Metadata" (November, 2005, Version 1.1)

Luciana Duranti, Principal Investigator; Terry Eastwood, Co-Investigator; Heather MacNeil, Research Assistant School of Library, Archival & Information Studies University of British Columbia Vancouver, B.C., 'The Preservation of the Integrity of Electronic Records', available in electronic format at <http://www.interpares.org/UBCProject/index.htm>

Dutch National Archives, 'Digital Preservation Testbed From digital volatility to digital permanence Preserving email' (The Hague, April 2003)

European Union

Documentation on Model for Electronic Record Management (MoReq) available in electronic format at <http://europa.eu.int/idabc/en/document/2631/5585>

International

BS ISO 15489-1:2001 Information and documentation. Records management. General available in electronic format at <http://www.bsi-global.com/ICT/Legal/bsiso15489-1.xalter>

InterPARES

The Long-term Preservation of Authentic Electronic Records: *Findings of the InterPARES Project* (2001) available in electronic format at http://www.interpares.org/ip1/ip1_index.cfm

US InterPARES Final Report, available in electronic format at <http://www.gseis.ucla.edu/us-interpares/pdf/InterPARES1FinalReport.pdf>

US InterPARES Interpreted A Guide to Findings on the Preservation of Authentic Electronic Records, available in electronic format at <http://www.gseis.ucla.edu/us-interpares/pdf/InterPARESInterpreted.pdf>

Brian Lavoie and Richard Gartner. 'Technology Watch Report' (Digital Preservation Coalition, September 2005)

The Sedona Conference

Best Practices Recommendations & Principles for Addressing Electronic Document Production A Project of The Sedona Conference® Working Group on Best Practices for Electronic Document Retention & Production (WG1) July 2005 Version

Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age A Project of The Sedona Conference® Working Group on Best Practices for Electronic Document Retention & Production September 2005

Understanding Metadata (NSIO, 2004) available in electronic format at http://www.niso.org/standards/std_resources.html

United Kingdom, The National Archives

Generic requirements for sustaining electronic information over time: 1 Defining the characteristics for authentic records

Generic requirements for sustaining electronic information over time: 2 Sustaining authentic and reliable records: management requirements

Generic requirements for sustaining electronic information over time: 3 Sustaining authentic and reliable records: technical requirements

Generic requirements for sustaining electronic information over time: 4 Guidance for categorising records to identify sustainable requirements

United States Department of Justice, 'Admissibility Of Electronically Filed Federal Records As Evidence' (October 1990)

NARA Code of Federal Regulations, Part 1234 - Electronic Records Management available in electronic format at <http://www.archives.gov/about/regulations/part-1234.html>

Some web sites of interest

Australia

Australasian Digital Recordkeeping Initiative

<http://www.adri.gov.au/>

Australian Partnership for Sustainable Repositories

<http://www.apsr.edu.au/>

Digital preservation software applications from the National Archives of Australia

<http://www.naa.gov.au/recordkeeping/preservation/digital/applications.html>

National Archives of Australia

<http://www.naa.gov.au/recordkeeping/default.html>

Records management, ISO 15489-1:2001, Standards Australia 2001

<http://www.saiglobal.com/shop/script/search.asp>

Recordkeeping Metadata Standard for Commonwealth Agencies, Version 1.0, National Archives of Australia, 1999

<http://www.naa.gov.au/recordkeeping/control/rkms/summary.htm>

Management of Electronic Records PROS 99/007 (Version 2), Victorian Electronic Records Strategy (VERS)

<http://www.prov.vic.gov.au/vers/standard/version2.htm>

Canada

Library and Archives of Canada

http://www.collectionscanada.ca/preservation/13_e.html

Archives of Ontario

<http://www.archives.gov.on.ca/>

Information Management Forum

http://www.imforumgi.gc.ca/tor-man/tor-man_e.asp?who=/&id=127

Records Management Institute

http://www.rmicanada.com/home_e.html

Treasury Board Secretariat

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/im-gi/siglist_e.asp

International

International Council on Archives

<http://www.ica.org/>

InterPARES 2 Project

<http://www.interpares.org/>

Ireland

Dublin Core Metadata Initiative

<http://dublincore.org/>

Netherlands

Nationaal Archief

<http://www.archief.nl/>

New Zealand

Archives New Zealand Te Rua Mahara o te Kāwanatanga

<http://www.archives.govt.nz/>

United Kingdom

Association for Information and Image Management

<http://www.aiim.org.uk>

Digital Curation Centre

<http://www.dcc.ac.uk>

Digital Preservation Coalition

<http://www.dpconline.org>

Electronic Resource Preservation and Access Network (ERPANET)

<http://www.erpanet.org>

Information Management Research Institute

http://online.unn.ac.uk/faculties/art/information_studies/Imri/rarea/rm/rmresearch.htm

International Records Management Trust

<http://www.irmt.org/contact.html>

The Joint Information Systems Committee (JISC) Digital Preservation and Records Metadata

<http://www.ukoln.ac.uk/metadata/>

Management Programme

http://www.jisc.ac.uk/index.cfm?name=programme_preservation

National Association for Information Management

<http://www.naim.uk.net>

National Preservation Office

<http://www.bl.uk/npo>

Nestor

<http://www.langzeitarchivierung.de/index.php>

Portal for electronic records

<http://www.nas.gov.uk/reckkeep/PDFs/ELECTRONIC%20RECORDS%20bibliography.pdf>

PREMIS (PREservation Metadata: Implementation Strategies) Working Group

<http://www.oclc.org/research/projects/pmwg/>

Public Record Office

<http://www.pro.gov.uk>

Records Management Society of Great Britain

<http://www.rms-gb.org.uk>

Society of Archivists

<http://www.archives.org.uk>

UK Data Archive

<http://www.data-archive.ac.uk>

United States of America

ARMA International

<http://www.arma.org/>

California Digital Library

http://www.cdlib.org/programs/digital_preservation.html

Council of State Archivists

<http://www.statearchivists.org/arc/index.htm>

Digital Document Quarterly

<http://home.pacbell.net/hgladney/ddq.htm>

US InterPARES

<http://www.gseis.ucla.edu/us-interpares/>

ISO Archiving Standards

<http://ssdoo.gsfc.nasa.gov/nost/isoas/>

Legal considerations in designing and implementing electronic processes: A guide for Federal Agencies (U. S. Department of Justice, November 2000)

<http://www.cybercrime.gov/eprocess.htm>

The National Archives

<http://www.archives.gov/preservation/>

The National Digital Information Infrastructure and Preservation Program

<http://www.digitalpreservation.gov/>

National Information Standards Organization

<http://www.niso.org/>

The Sedona Conference

<http://www.thesedonaconference.org/>

The University of Pittsburgh School of Information Sciences

<http://www2.sis.pitt.edu/~rcox/FunReqs.htm>

The University of Pittsburgh School of Information Sciences web site has the following statement:

‘The Functional Requirements for Evidence in Recordkeeping was a project administered out of the University of Pittsburgh School of Information Sciences between 1992 and 1996 and funded by the National Historical Publications and Records Commission. Due to a technical glitch at the School the Web site with the working files of this project was destroyed, but since the Web site has not been updated since 1996 when the Project ended individuals interested in the project and use of the site can access it through the Internet Archive.’

ⁱ http://en.wikipedia.org/wiki/Analog_computer.

ⁱⁱ <http://en.wikipedia.org/wiki/Digital>.

ⁱⁱⁱ http://en.wikipedia.org/wiki/Electronic_document.

^{iv} One definition of database is included in the Copyright, Designs and Patents Act 1988. The Copyright and Rights in Databases Regulations 1997 (Statutory Instrument 1997 No. 3032) amended the Copyright, Designs and Patents Act 1988 to provide for the meaning of ‘database’, by inserting section 3A of the Regulations below section 3 of the Act, as follows:

3A. - (1) In this Part "database" means a collection of independent works, data or other materials which –

(a) are arranged in a systematic or methodical way, and

(b) are individually accessible by electronic or other means.

(2) For the purposes of this Part a literary work consisting of a database is original if, and only if, by reason of the selection or arrangement of the contents of the database the database constitutes the author's own intellectual creation."

^v Civil Procedure Rules, rule 32.19(1).

^{vi} For further comments, see John D. Gregory, ‘Authentication Rules and Electronic Records’, *The Canadian Bar Review*, Volume 81, 2002, pp 531 – 533.

vii An example from the United States of America is that of *Scholastic, Inc., J. K. Rowling and Time Warner Entertainment Company, L.P. v Stouffer* 221 F.Supp.2d 425 (S.D.N.Y. 2002).

viii John D. Gregory, 'Authentication Rules and Electronic Records', p 533.

ix The State of Israel v van (John) Demjanjuk, Criminal Cases (Jerusalem) 373/86 a full transcript of which is published in *The Demjanjuk Trial*, (Israel Bar Publishing House, 1991); Yoram Sheftel, *Show Trial*, (Victor Gollancz, 1994); Tom Teicholz, *The Trial of Ivan the Terrible*, (Futura, 1990); Williem S. Wagenaar, *Identifying Ivan*, (Harvester – Wheatsheaf, 1988).

x Section 40(1).

xi Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* (Centre for Commercial Studies Queen Mary and Westfield College, 1996) pp 9-15.

xii [1908] 2 KB 333.

xiii [1908] 2 KB 333 at 340. See *Phipson on Evidence* (16th Edition, 2005) para 41-02 for a more detailed discussion.

xiv [1975] Ch 185; [1974] 3 WLR 221; [1974] 2 All ER 465; 118 SJ 548 Ch D; 232 EG 333, Chancery Division.

xv Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* Chapter 1 for a more detailed treatment.

xvi See *Phipson on Evidence* (16th Edition, 2005) para 41-02 for a more detailed discussion.

xvii Charles Hollander QC and Tom Adam *Documentary Evidence* (Sweet & Maxwell, 2000) p 79.

xviii Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* pp 83 - 84 for other statutory definitions and further comments.

xix Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* pp 94 – 102.

xx The Model Law on Electronic Commerce was adopted by the Commission on 12 June 1996, following its 605th meeting, which in turn was adopted by the General Assembly in Resolution 51/162 at its 85th plenary meeting on 16 December 1996, and includes an additional article 5 *bis* as adopted by the Commission at its 31st meeting in June 1998.

xxi Guide to Enactment paragraph 48.

xxii The reader is directed to a very helpful discussion by Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* pp 136 – 147. The reader is also referred to ISO 15489 Information and documentation -- Records management and the definitions cited therein.

xxiii Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* Chapter 4.

^{xxiv} [1896] 1 QB 309; 65 LJMC 74; 74 LT 254; 44 WR 318; 18 Cox 285; 60 JP 519.

^{xxv} [1896] 1 QB 309 at 314.

^{xxvi} [1896] 1 QB 309 at 321.

^{xxvii} Chris Reed *Digital Information Law Electronic Documents and Requirements of Form* p 186.

^{xxviii} (OJ L13/12 19 January 2000).

^{xxix} 457 N.W.2d (Iowa App. 1990).

^{xxx} Case No 1803325/97.

^{xxxi} The National Archives, undated, paragraph 3.1.4.

^{xxxii} IV. Conclusion, (U. S. Department of Justice, October 1990) available in electronic format at <http://www.lectlaw.com/files/crf03.htm>.

^{xxxiii} 336 B.R. 437 (9th Cir. BAP 2005); 2005 WL 3609376; 06 Cal. Daily Op. Serv. 146; 2006 Daily Journal D.A.R. 169 (B.A.P. 9th Cir. Dec 16, 2005).

^{xxxiv} At 445 [15].

^{xxxv} Edward J. Imwinkelried, *Evidentiary Foundations* (6th edn, 2005) paragraph 4.09[4][c].

^{xxxvi} The hardware can be important. For instance, the jazz club Ronnie Scotts, based in Soho, London, was refurbished in 2005 – 2006. As each part of the club was renovated, so large numbers of recordings of jazz musicians and singers, such as Dizzy Gillespie, Ella Fitzgerald, Chet Baker, Sarah Vaughan and Buddy Rich, recorded during live performances, were discovered. Some of the recordings were made on tapes that required machines that were no longer in the possession of the club, so they will have to find a specialist company that has retained the relevant type of machine in order to re-play the tapes: report by Bob Sherwood, *Financial Times*, Wednesday June 28, 2006, 1.

^{xxxvii} 1 F.3d 1274 (D.C. Cir. 1993).

^{xxxviii} 184 F.3d 900 (D.C. Cir. 1999).

^{xxxix} Paragraph 3.1.7.

^{xl} Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation' *Digital Evidence Journal*, 2006 Volume 3 Number 1, 38 – 42.

^{xli} How long a document will need to be retained depends on a number of factors. In order: periods of time set out in legislation, periods of time determined by regulations issued under the authority of legislation; periods of time defined by regulatory authorities; periods of time defined by industry best practice. For a discussion in the UK context, see Stephen Mason, *E-Mail, Networks and the Internet: A Concise Guide to Compliance with the Law* (xpl publishing, 6th edn, 2006) Chapter 7.

^{xlii} <http://www.dpconline.org/graphics/intro/definitions.html>.

^{xliii} Peter B, Hurlle, 'Archival Authenticity in a Digital Age' in Authenticity in a Digital Environment (Council of Library and Information Resources, May 2000) pp 8-9.

^{xliv} For further information on the Heiner affair, see:
<http://www.caldeson.com/RIMOS/summary.html> and the links on this web site;
Australian Society of Archivists Position Statement on the Heiner Affair at
<http://www.archivists.org.au/pubs/positionpapers/heiner.html> and the Senate Select
Committee on the Lindeberg Grievance at
http://www.aph.gov.au/Senate/committee/lindeberg_ctte/ctte_info/index.htm.

Funds for this study were provided by



The ARMA International Educational Foundation

The ARMA International Educational Foundation is the non-profit, (501(c)3, affiliate of ARMA International, the primary professional association for the records and information profession in the world.

Mission

The ARMA International Educational Foundation supports education and research initiatives that promote the advancement of both information managers and the information management profession. Recorded information is the lifeblood of the modern organization, but rarely is it treated as a critical asset, primarily because there is little quality research to create the comprehensive body of knowledge required to support information management as a profession. The AIEF purpose is to answer that need by soliciting funds for this research and then providing a vehicle through which conclusions can be tested, documented and communicated to the information management community.

If you found value in this publication, please consider making a financial contribution to the Endowment Fund of the Foundation. This can be accomplished by visiting the Foundation's web site, www.armaedfoundation.org, or by contacting

Foundation Administrator
ARMA Int'l Educational Foundation
1609 Terrie Drive
Pittsburgh PA 15241
USA

Additional information about the Foundation can be found at



The National Database of Non-profit Organizations

http://www.guidestar.org/search/report/gsearch_report.jsp?ein=31-1556655

Comments about this publication and suggestions for further research are welcome. Please direct your inquiry to the Foundation Administrator.