Society of Construction Arbitrators

Conference – Edinburgh May 2009

E-Discovery

by

David J Cartwright
MA, FRICS, FCIArb, FAMINZ(Arb)

Contents

1. Introduction

I was invited to present this paper on e-discovery because of my interest in computers, data management and business governance as well as some recent arbitral experience in the use of electronic documentation.

You will be pleased to hear that I do not intend to visit all the nuances of the disclosure process within common law jurisdictions. Instead the paper is a canter through relevant aspects of discovery and disclosure in a way which hopefully teases out some of the difficulties and areas of concern for arbitrators when faced with applications for e-disclosure or discovery.

Whilst both arbitration and court rules make provision for discovery, the court rules generally provide a better indication of how the process has developed from which arbitration can draw some assistance. Particularly as most advocates, in an effort to persuade the arbitrator to issue directions, naturally base their applications for discovery on court decisions.

Therefore, I will refer to various court rules, cases and court practice notes on electronic disclosure from various jurisdictions in order to illustrate some pitfalls. I will also be touching on aspects of technology and how various jurisdictions are endeavouring to meet the challenge of the digital age and how indeed new concepts and technologies are said to be assisting society and investigators to obtain the truth.

By way of introduction I felt it was important to consider the development of document production on some form of timeline.

2. Historical Overview of Document Production

The technology used to produce documents has evolved significantly throughout history. While a great deal can be said about the changes in ancient production technologies including papyrus, palm leaves, stone tablets and marking devices ranging from quills to chisels; the modern form of the document has evolved largely under the influence of printing and reproduction technologies.

Prior to the invention of the printing press a huge effort was required to faithfully produce copies of documents by hand[1] which severely limited both the number of documents available, and access to the information contained therein. The process was improved slightly by early printing devices but the effort to set type and prepare a document for reproduction was still high, although many high fidelity copies could be produced. However, a big leap occurred in 1440 with the invention of the Gutenberg printing press which enabled the mass production of faithful copies of documents, and hence the increased availability of information.

Many old documents survive today which illustrates the longevity of the technology of their day, subject of course to the storage methods adopted. For example we still find cave pictures from prehistoric times[2] and documents dating from around 6th & 9th centuries[3]. Some of the more well known historical documents are the Domesday Book which records the great survey of England completed in 1086[4] and the Magna Carta of 1215.[5] Both these documents can still be read today, but I doubt their authors considered the life of the documents or whether people would be able to understand or even read them over 900 years later. But one important point to note is that these documents had a very limited circulation due to the restrictions of hand produced documents, and perhaps the materials were more robust and because of the limited quantity, greater care was taken with storage.

The limited circulation problem was largely overcome some four centuries later by the Gutenberg Press but it took another 400 years before there was any significant change in the way paper documents were produced. This change occurred in 1867 when Christopher Sholes[6] invented a typewriter with the QWERTY keyboard layout[7]

[1] Magna Carta was written on parchment, not on paper. Parchment was the normal writing material in England until the end of the Middle Ages. It was made from sheepskin which was soaked in a bath of lime, then stretched on a frame to dry under tension. When it was dry, the skin was scraped with a curved knife to produce a smooth writing surface for the scribes, who wrote their text with a quill pen. http://www.bl.uk/treasures/magnacarta/basics/basics.html

[2] Lacaux, France. The original caves are not for public display but a reproduction is available to view nearby.

[3] Book of Kells held at Trinity College Library which consists of some 340 pages as an illuminated manuscript in Latin, containing the four Gospels of the New Testament from and compiled from England, Scotland and Ireland.

[4] Executed for William I of England, William the Conqueror. The first draft was completed in August 1086 and contained records for 13,418 settlements in the English counties south of the rivers Ribble and Tees (the border with Scotland at the time). http://www.domesdaybook.co.uk/

[5] King John of England agreed, in 1215, to the demands of his barons and authorized that handwritten copies of Magna Carta be prepared on parchment, affixed with his seal, and publicly read throughout the realm. http://www.bl.uk/treasures/magnacarta/basics/basics.html

[6] A newspaper editor in Milwaukee USA.

However having spent a further 6 years developing it he sold it to Remington in 1874[8].

I should also mention that during the same period in the 19th Century, an English Engineer considered by some to be the father of computing, Charles Babbage (1791-1871), was designing number crunching machines to avoid the boredom and inaccuracies in reading paper tables. It is unfortunate that although he designed various devices, a full working version was not completed until 2002[9].

2.1. Recent Developments

However, in the 21st century, some 135 years later, we are still basically using paper and the same typewriter keyboard layout to produce documents, although the production method has changed. We also seem more removed from the output. When you use a pen or pencil on a piece of paper you are in direct contact with the medium and create a personal symbol to create a picture, word or a number. The typewriter on the other hand is one step removed and creates an impersonal symbol on the paper but this symbol is a personal symbol to that typewriter. This is because a mechanical device, such as a typewriter, is designed and manufactured with tolerances and hence as no two typewriters are absolutely identical the symbol is unique to each machine.

Today's technology has advanced with the use of an electronic device to process numbers – calculators and words – word processors, but in the initial stages these devices were so costly that only large business and governments could afford to run them. To put this into perspective, some 40 years ago when typewriters and pencils were in general use electronic machines were still in their infancy. At that time whilst at university we were designing machines that could calculate formulae and produce graphs on XY plotters, but within 5 years pocket calculators were available at affordable prices and within 10 years personal computers were also available.

We can see from that the new electronic age and the ability to produce documents without using paper and pencil became more acceptable in everyday life. These technologies developed both in the home and in the workplace, some of the more significant developments you may recall were:

1975 Wang Office Information System – word processor multi user system[10].

[7] Patent was registered October 1867.

[8] The basic keyboard layout has basically remained the same since its invention. The first model was released in 1874 . One of Remington's marketing adjustments was to include 'R' in the top row so that salesmen could type 'typewriter' from one row. Apparently there are others differences with the modern layout if you compare them with the patent of 1878, but this varies with individual regions.

[9] An English Engineer whose designs remained a historical curiosity for over 150 years. Finally, in 2002, the first full-size Babbage Engine (Difference Engine no 2), built faithfully to the original designs, was completed at the Science Museum in London, the culmination of a seventeen year project. The Engine consists of 8,000 parts, weighs 5 tons and measures eleven feet long and seven feet high. It works as Babbage intended, and brings to a close an anguished chapter in the prehistory of computing. http://www.computerhistory.org/babbage/overview/

[10] This was later succeeded with WANG Office Information System called WANG OIS in 1977. [These were lower in power than the IBM PC which came out in 1981]. WANG produced separate lines for word processing and data processing albeit they used similar technologies. Interestingly WANG's main business was mini computers and mini frame computers but this lost out to micro

1980 Sir Clive Sinclair released his home PC, the ZX 80[11].
1981 IBM Personal Computer[12]
1982 Compaq Portable[13]
1982 IBM with a Hard Drive[14]
1982 IBM Home PC[15]
1984 Amstrad produced the PCW8512 Word Processor.
1986 Amstrad took over Sinclair.

During this period people were experimenting in the home, encouraged by the ZX80 and the BBC home computer[16], with a computer language called 'Basic'[17]. By comparison, in the workplace there was movement away from typewriters with the advent of WANG word processor which was an instant success. However, the market for standalone word processing systems collapsed with the introduction of personal computers which meant other manufacturers[18] entered the market place. This was partly possible due to IBM's[19] decision to adopt Microsoft as its operating software[20] and to use open architecture which permitted third party developments that were 'IBM compatible'.

With this explosion in technology and the greater awareness of business and consumers, consideration had to be given to the ease of use and storage mediums. The intended storage medium for the original IBM[21] was a compact cassette but as DOS[22] was not available for this medium, floppy disks took over, with most IBM's at that

computers or PC's like IBM, HP, Apple. Nevertheless the support for WANG's mini frame operating system lasted until 2008. http://www.computermuseum.li/Testpage/WangGetronics.htm

[11] It was offered in both a kit form at £50 and ready built at £100 which gives an indication of the state of knowledge or awareness of the consumer market. Later the Spectrum was introduced with either a tape drive or floppy disc. At that time there were two other manufacturers, Commodore and Amstrad, and in an attempt to take market share, Amstrad introduced the CPC464 in 1984.

[12] IBM PC using 'Multimate' replicated the functions of WANG word processor. http://digitize.textfiles.com/items/1982-ibm-personal-computer

[13] Compaq launched a portable in November 1982.

[14] IBM launched the XT which was the first IBM PC with an internal hard drive (10mb). http://en.wikipedia/org/wiki/IBM_Personal_Computer

[15] The first floppy based home computer the PCjr.

[16] This computer was produced by Acorn from 1980 and derived is name from the BBC because the BBC decided to start a computer literacy television series. The network realised that, with more powerful and increasingly inexpensive microcomputers, it would soon be possible to create them with enough computing power to offer their owners personal hands-on experience with microcomputers at an affordable price (about £400). http://www.old-computers.com/museum/computer.asp?c=29

[17] Computer programming language developed in the USA in the 1960's by John G. Kemeny and Thomas E. Kurtz b1928 http://www.britannica.com/EBchecked/topic/54939/BASIC

[18] Other US manufacturers were in the 'personal computer' market with Xerox PARC Alto using the phrase in 1972 but due to the success of IBM Personal Computer, which was introduced on 12th August 1981 (Model 5150 – CPU speed 4.77Mhz & memory 16kb to 256kb) the term has come to mean compatibility with IBM PC products. Until then IBM had produced PCs for professional and scientific problem solvers, not business users or hobby use, at a cost up to $20,000.00. http://en.wikipedia/org/wiki/IBM_Personal_Computer

[19] IBM did not expect personal computers to last and so did not restrict the agreement with Microsoft. If they did had the OS system may not have been so widely used.

[20] In lieu of its own IBM OS.

[21] 5150.

[22] Disk operating software.

time having 2 No. 5 ½ " floppy disk drives[23]. However, IBM exited the desktop PC market in 2004 when it sold out to Lenovo.

Today most businesses run networked computers, with or without hard drives using an operating system of either a Microsoft derivative, Linux or Novell. Nearly all homes have a computer of at least the same power as the business PC and with the media revolution, homes now have networks. These networks are often linked by cables or wirelessly or via the internet or VPN's[24] to other networks to exchange information. This information may be in the form of data, a communication, monitoring (cameras) or a means of controlling other equipment[25].

I have tried to encapsulate the development of computer technology to illustrate how it has grown and become an integral part of life[26]. It seems to be accepted as a necessity for home use with Internet banking, e-mails, telephone calls via Skype and instant messaging[27]. This rapid growth has, to some extent, been driven by the entertainment industry as the increase in games and the power required to run the games has driven the development of new processing power, faster memory and faster and larger hard drives. In 1950 Alan Turing wrote a paper called 'Computing Machinery and Intelligence' [28] in which he predicted that by the turn of the 20th century computers would have a billion[29] words of memory. I am sure this rate of development could not have been envisaged by Babbage, although Turing was clearly a visionary as he recognised the vast storage potential. Both these inventors had been designing and working on machines that crunched numbers and deciphered data. The introduction of the transistor and integrated circuit lead to word processors and then to computers which held and processed data very quickly.

The technology has been transferred to mobile phones which can create, edit and transmit documents to other phones or computers, which probably makes them more powerful than PCs of even twenty years ago. These changes in technology and the way people have used computers has increased the need for better protection, security and management of intellectual property to prevent the loss of electronic data even by post or on a train.

[23] One for the operating system and one for the data (160kb or 360kb). This technology is now largely obsolete.
[24] Virtual Private Networks.
[25] Used as surveillance or controlling building environments.
[26] W Abel and B Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems" – a case report on BVerfG, NJW 2008, 822", (2009) 6:1 SCRIPTed 106, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp Para 5 Conclusion. "*By creating the new fundamental right in the confidentiality and integrity of information technology systems the Court has, for the first time, recognised that information technology not only plays an important role in people's lives as an add-on or extension to live in the physical world, but also that an increasing number of people "live" online. The Internet has become a living space, where people make friends, form societies and exchange information, and the Court has acknowledged that existing legislation is insufficient to adequately protect citizens from state violations of this digital environment. The "digital citizen" has, as a result of this case, come a step closer*."
[27] Windows Live or Skype.
[28] http://www.turing.org.uk/turing/scrapbook/test.html
[29] Quoted at a time when a billion was a million million. In today's terms it would be 1,000 billion words.

So what has this to do with resolution of disputes? Simply that a large proportion of records are no longer stored in paper form and hence procedures are required to enable the data to be preserved in a manner that is readable so it can be produced as a matter of record in any legal proceeding. The increased capability of production techniques and availability for transmission means an increased quantity of records in an ever increasing number of formats, all of which need to be managed.

2.2. What is a Document?

Whilst I am sure that most legal professionals are fully familiar with the process of discovery I will, for the sake of completeness, look at some basic points before we apply these principles, if indeed they are the correct principles to apply, to electronic documentation.

First, let us consider the term 'document' and how various jurisdictions and/or rules currently define documents but let's start with the UK Civil Procedure Rules[30] which define the meaning of 'documents' as:

> '*anything in which information of any description is recorded*' and
>
> 'copy' means, in relation to a document,
>
> '*anything onto which information recorded in the document has been copied by what ever means and whether directly or indirectly*'.

By way of example to show how other jurisdictions have defined documents I would like to refer you to various Rules of Court and Evidence in Canada.

In January 2005, the Ontario's Rules of Civil Procedure were amended to expand the definition of 'document' to include:

> *" a sound recording, videotape, film, photograph, chart, map, plan, survey, book of account and data and information in electronic form;"*[31]

British Columbia's Supreme Court Rules[32] and the Alberta Rules of Court[33] provide for the inclusion of electronic documents within their definitions of document and record, respectively.

Rule 1(8) of the British Columbia Supreme Court Rules provides that a 'document':

> "*has an extended meaning and includes a photograph, film, recording of sound, any record of a permanent or semi-permanent character any information recorded or stored by means of any device"*.

Part 13 s186 of the Alberta Rules of Court say that a 'record' includes:

[30] 2009 Rule 31.4
[31] RRO 1990 Regulation 194; r30.01 (1) (a)
[32] B.C Reg 221/90. Amendment 2009
[33] Alberta Regulation 221/2009 AR 390/68 s185.

> *"the physical representation or record of any information, data or other thing that is capable of being represented or reproduced visually or by sound or both".*

These definitions are consistent with but not identical to the definitions in the Evidence Acts of British Columbia[34], Alberta,[35] and Ontario[36], as well as the Canadian Evidence Act[37]. However, the Canadian Evidence Act defines an 'electronic document' as:

> "*data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data*".

In addition, various territories have enacted specific Electronic Evidence Acts[38] which are more in the terms of the Canadian Evidence Act. However, British Columbia[39] issued, in relation to Rule 1(8), a Practice Direction on Electronic Evidence which states that a document in writing includes:

> *"a. any book, map, plan, graph, or drawing;*
>
> *b. any photograph;*
>
> *c. any label, marking, or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means whatsoever;*
>
> *d. any disc, tape, sound track, or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom;*
>
> *e. any film (including microfilm), negative, tape, or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and*
>
> *f. anything whatsoever on which is marked any words, figures, letters, or symbols that are capable of carrying a definite meaning to persons conversant with them."*

[34] Evidence Act, R.S.B.C. 1996, c124. s.42
[35] Evidence Act, R.S.A. 2000, cA18. s41.1 (b)
[36] Evidence Act, R.S.O. 1990, cE.23 s.34.1(1).
[37] Canada Evidence Act, R.S.C. 1985, cC-5, s31.8
[38] Foe example the Yukon Territory enacted the Electronic Evidence Act R.S.Y 2002 c67
[39] July 2006; http://www.commonwealthlegal.com/pdf/ElectronicEvidenceJuly2006.pdf

2.3. IBA Rules

From these Acts and Rules it is difficult to see how anything could escape the scope of latter definition. However, the IBA Rules on the Taking of Evidence in International Commercial Arbitration [40] (the "IBA Rules of Evidence") define 'documents' in perhaps a more concise form in Article 1 as:

> "*a writing of any kind, whether recorded on paper, electronic means, audio or visual recordings or any other mechanical or electronic means of storing or recording information*".

The IBA Rules of Evidence clearly take into account the various classifications of documents as identified for example in the CPR and the Canadian Civil Evidence Act, and thus for the purposes of this paper I will adopt this concise definition. The question remains how we deal with documents in this jurisdiction but before I move on, I thought I would provide some examples of recorded information.

2.4. Examples of Documents/Records

Examples of stored information that have been construed as documents for the purposes of the UK CPR rule[41], include:

Type of Document	Case Reference	Notes
Audio Recordings	*Grant v South Western and County Properties Ltd* [1975] CH 185	In which the derivation of the word was pointed out to be from the Latin documentum which means "some thing that instructs or provides information".
Videotape	*Garcin v Amerindo Investment Advisers Ltd* [1991] 4 all ER 655	
Plans	*Hayes v Brown* [1920] 1KB 250 at 252	
Inscriptions on a Wall	*Roscoe v Groundsell* [1903] 20 PLR	
Computer Files	*Derby & Co Ltd v Weldon (No. 9)* [1991] 1WLR 652 at 657-658	This included databases-so long as there is information capable of being retrieved.

[40] Published and produced by the International Bar Association and adopted on 1st June 1999. ISBN 0 948711 54X: 2006

[41] As listed in the editorial to White Book 2008; see pt 31.4.1 p771 para 3

Type of Document	Case Reference	Notes
Hard Disk of a Computer	*Alliance and Leicester Building Society v The Ghahremani* [1992] RVR 198 at 199	
Computer Databases	*Marlton v Tectronix UK Holdings* [2003] EWHC 383	
Computer Software	*Format Communications v ITT (UK) Ltd* [1983] FSR 473	

3. History of Discovery

Nearly all the references that I have considered for this paper refer to the well known case of '*The Compagnie Financiere Et Commerciale Du Pacifique v The Peruvian Guano Company*[42]. This case shaped the subsequent rules of the Supreme Court[43] and the Civil Procedure Rules in the UK and other jurisdictions.

For those familiar with the famous passage by Brett LJ but unfamiliar with the background of this case I thought it would be interesting to give an outline. The defendants claimed discovery of documents which were disclosed in the plaintiff's minute book included in the original affidavit. The book referred to documents including draft arrangements, board meetings, and communications between various parties and it was these documents that were sought. The Court of Appeal in overturning the first instance decision held that the documents were to be disclosed as they were not limited to documents which would be admissible in evidence nor to those which would prove or disprove any matter in question.

The much quoted passage from this case refers to any documents which, it is reasonable to suppose,

> "*contains information which may enable the party (applying for discovery) either to advance his own case or to damage that of his adversary, if it is a document which may fairly lead him to a train of enquiry which may have either of these two consequences*".[44]

These principles were encapsulated in the UK Supreme Court Practice Order 24[45] but this changed following the New Civil Procedure Rules[46] ("CPR") which came into effect on 26th April 1999. The CPR contained an overriding objective which included enabling the Courts to deal with cases justly[47], saving expenses and dealing with cases in a proportionate manner.

3.1. UK Civil Procedure Rules

I will now turn to the disclosure aspects of the CPR rules which changed the format of litigation in the UK, and have been adopted in other jurisdictions, where they relate to the disclosure and inspection of documents.

In providing rules about the disclosure and inspection of documents CPR defines disclosure[48] as when:

[42] 11QBD 55 (1882) CA.
[43] The case was based on the 1875 Rules of the Supreme Court.
[44] p 63: Supreme Court Practice - White Book 1988, Vol 1, p 413, O24/2/5
[45] Ibid Order 24 r1 so that after the close of pleadings in an action there may be discovery by the parties to the action of the documents, which are or have been in their possession, custody or power relating to matters in question in the action.
[46] Lord Woolfe Reforms.
[47] Pt 31
[48] CPR 31.2

> '*a party discloses a document by stating that the document*[49] *exists or has existed'.*

Nevertheless, the parties have an obligation to disclose documents[50] which is anything that records information of any description and thus it includes all electronic documents, including e-mails and other communications, word processing documents and databases.[51] This includes documents readily accessible from computer systems and other electronic devices and media, as well as material stored on servers and backup systems and electronic documents which have been apparently deleted (a record of which will often remain on the computer systems).

Failure to deliver up computers and the deliberate deletion of files from a computer in contravention of a search order may amount to a contempt of court[52]. There could be a tension here with the parties' internal data management policies but I will refer to that later.

Any search has to be reasonable, and helpfully the CPR[53] sets out the factors to decide the reasonableness of such search, as referred to in Practice Direction 31PD.2A.4 (c) as:

a) number of documents involved;
b) the nature and complexity of the proceedings;
c) the ease and expense of retrieval of any particular document; and
d) the significance of any document which is likely to be located.

It may be reasonable to search for some or all of other parties' documents on some or all of its electronic systems. In other cases it may be reasonable to find certain documents by means of keyword searches or time span. The important factor is for the parties to agree as far as possible these limitations. The potential for a great volume of electronic documents means that the issues of scope and reasonableness of the search need to be carefully considered.[54] The rules are intended to avoid excesses of effort, resources and costs in relation to disclosure and their associated costs.

Hence, the *Peruvian Guano* principles have been narrowed if not discarded[55] by the new CPR and indeed by other jurisdictions, as it is a commonly held view that discovery, particularly in the USA is extremely expensive and time consuming. This has lead to various organisations being formed to consider the ramifications of the electronic age within the litigation process. I will return to this later.

[49] Under r31.4 the meaning of 'documents' is defined as 'anything in which information of any description is recorded' and 'copy' means, in relation to a document, 'anything onto which information recorded in the document has been copied by what ever means and whether directly or indirectly'
[50] Defined in CPR 31.4
[51] CPR Practice Direction pt 31.2A .1
[52] LTE Scientific Ltd v Thomas [2005] EWHC 7 QB
[53] R 31.7.2
[54] Hands v Morrison Construction Services Ltd [2006] EWHC 218
[55] The White Book 2008 editorial to CPR 31.0.4, para 4. Also previously Peruvian Guano was criticized in the case of O Co. v. M. Co. [1996] 2 Lloyd's Rep.347, when the Court said that the principles were never intended to justify demands for disclosure of documents at the far end of the spectrum of materiality which on the face of it were unrelated to the pleaded case of the plaintiff or defendant and which were required for purely speculative investigation.

3.2. Privilege

It seems that no matter how careful one is it occasionally happens that privileged documents are included in disclosure by mistake. CPR 31.20 concerns the restriction on the use of the privileged document inspection which has been inadvertently disclosed.

There have been several cases on this point in various jurisdictions. One of the more recent was heard in the Court of Maryland, *Victor Stanley Inc v Creative Pipe Inc et al*[56]. In this case the argument was over 165 No. documents which were inadvertently disclosed electronically and on the facts the Court found the defendant had waived its privilege.

So when documents have been disclosed in proceedings are they privileged? Under CPR, subsequent use of disclosed documents is restricted by CPR 31.22 which specifies the clear exceptions to the general rule that '*any document disclosed in proceedings may only be used for the purposes of those proceedings*'.

As regards arbitration proceedings, it was held in *Hassneh Insurance Company of Israel v Stewart J Mew*[57], that there was an implied undertaking not to use disclosed documents for purposes other than the arbitration in which they are disclosed. The qualification to such an implied undertaking, namely that the award might be disclosed as of right if it was reasonably necessary for one party to disclose it for the purposes of the establishment of that party's right against the third party, either in order to found a defence or as the basis for a cause of action, was further considered in *Insurance Company v Lloyd's Syndicate*[58]. Here the Court held that 'reasonably necessary' covered only the case where the right in question could not been enforced or protected unless the award and reasons were disclosed to a stranger to the arbitration. Clearly, on this basis the award is not limited to just those 'private' arbitration proceedings[59].

3.3. Disclosure Practice in CPR

The emphasis in the CPR is to encourage party agreement at an early stage[60] in adopting the right process by discussing the format in which these documents will be provided for inspection. The CPR and Practice Direction [61] requires the parties prior to the first case management conference to discuss any issues that may arise regarding searches[62] and the preservation of electronic documents. This may involve providing the categories of electronic documents within their control, the computer systems,

[56] [2008] MJG-06-2662
[57] [1993] 2 Lloyds Rep 245
[58] [1995] 1 Lloyd's Rep 272
[59] UNCITRAL r25.4 states 'hearings in camera unless parties agree otherwise' (United Nations Commission on International Trade Law).
[60] Practice Direction Para 2A.3
[61] Practice Direction 31.2A
[62] Practice Direction Para 2A.5 refers to reasonable search and notes that there may be other forms of electronic search that may be appropriate in the circumstances.

electronic devices and media on which any relevant documents may be held or stored. If there is any difficulty the matter must be brought to the judge for a decision at the earliest practical date.

This procedure is reflected in the Pre-Action Protocol for Construction and Engineering Disputes[63] and the Technology and Construction Court Guide[64]. The latter also refers to the Admiralty and Commercial Court guide concerning electronic disclosure and to TeCSA IT protocol[65].

To reinforce the position the parties are required to give a Disclosure Statement[66] which requires a statement to the effect that a reasonable and proportionate search has been carried out to locate all the documents which are required to be disclosed. The statement includes a list of documents which identify those documents which were not searched. The practice note also provides a helpful list of sources namely, documents contained on or created by the parties on or in:

> "*PCs, portable data storage, media, databases, servers, backup tapes, offsite storage, mobile phones, laptops, notebooks, handheld devices, PDA devices*".

Whilst this is a fairly comprehensive list, one has to bear in mind the overriding objective[67] which refers to making use of technology in terms of the court's duty to actively manage the cases and indeed several courts are running pilot schemes but it still raises the question, whether with technology is expert evidence needed on the retrieval side and at what cost?

In the Canadian case of *Prism Hospital Software Ltd v Hospital Medical Research Institute,*[68] files of deleted information recovered from computer disks by use of specialist software were held to be documents contained on magnetic media for the purposes of the relevant Evidence Act. In this case the party had disclosed the hard disks and tapes and allowed inspection by examination of the media itself. Inspection was carried out by the principal of the inspecting party who was very knowledgeable about computers. By the application of software he was able to recover information from previously deleted material and all the recovered information was admitted by the court, but it was argued that this evidence was expert evidence. The fact that knowledge of computers was required to recover the files and then to read them by means of a computer program did not mean that the evidence concerning the recovered files was expert opinion. The court explained that the skill and knowledge necessary to restore deleted documents is no longer rare and once restored, the documents could be read in the normal manner. This reflects the court's acceptance of restored data as being a reliable and sometimes a required source of relevant evidence.

But what of data management policies and costs of maintaining a system to offer protection against disclosure and the cost of disclosure?

---

[63] April 2007
[64] 2nd edn, 3rd October 2005 revised 1st October 2007
[65] April 2003, para 11.2.3
[66] Practice Direction 2A.9
[67] CPR r 1.4 (2) (k)
[68] [1992] 2WWR 157 (British Columbia Superior Court)

Cost is always at the forefront of people's minds, and from the point of view of this paper, disclosure raises some very interesting issues and basic questions on the source of the documents, such as;

- What sources are possibly relevant and over what date range?
- Which personnel matter and who will have the key documents?
- Where and how are the documents stored?
- How easy are they to access:
    - The media?
    - The software?
    - The data in which jurisdiction?
- Who knows about their existence?
- Which of the documents are actually relevant to the issues in the case?
- Is it likely that the parties will have concealed documents?
- What are the likely costs involved? consider a cost to value exercise.
- Consideration of the end user - the tribunal.

All these, in my submission, are important considerations, and should be part of the case management process, particularly when you consider that the CPR expects the use of technology to help reduce the costs. Does this mean that all legal professions will have to develop a new skill base?

In a Practice Note for the Australian Federal Court[69], for example, the court requires legal practitioners to be appraised on the basic capabilities of modern technology in so far as it relates to this Practice Note or, where they are not so appraised, to ensure they have access to advisers who have the necessary skills and experience, known as eRegistrars[70].

The lengths parties seem willing to go in broad terms to obtain documents without making any attempt to agree procedures in advance are indicated by the Irish case of *Judith Keane v Aer Rianta.*[71] In this case the plaintiff sought damages for falling off an alleged defective chair and sought amongst other documents "*all documentation of whatsoever nature relating to the make and type of chair provided for use by the plaintiff on the date of the accident*". The Court noted that this request 'looked impressive' but that on close examination it realised that the proof of the make and type of chair would not prove a defect. It concluded that the only issue was whether the fall was caused by the plaintiff's own carelessness or of a sort complained of by others. In the end it only awarded discovery of written complaints made by staff previously on chairs during the 18 month period prior to the accident. So clearly the Court took a proportional approach.

[69] Practice note 17 para 10; 29th January 2009
http://www.fedcourt.gov.au/how/practice_notes_cj17.htm
[70] Practice Note 17 para 10; 29th January 2009
[71] [2007] [2004 No 8651 P]

3.4. Summary

Under the new procedures it is apparent that in the UK and other jurisdictions the judge is clearly more involved in the case management; for example:

- In the UK he has a duty, based on the overriding objective, to use technology and the court resources;
- The limitation on disclosure means that the judge is implicated or involved in the decisions on what to leave out;
- The judge must have the facts in front of him on which to base his decision.

This can of itself increase the cost of litigation as recently discussed in an article in The Times where Judge Charles Harris QC[72] and Lawrence West, QC, Henderson Chambers[73] criticised the discovery process, concluding that it was very front cost heavy.

So you may ask yourself whether the CPR has achieved its aims and objectives to save costs and if not, whether this will lead to parties referring more matters to arbitration. Only time will tell.

[72] Source Times Online 16th April 2009
[73] Source Times Online 9th April 2009

4. Electronic Documents

4.1. Terminology

Having discussed the various rules and defined disclosure and documents we need to have an understanding on how technology can assist the process.

First of all, let us consider some basic statistics on the volume of documents and the storage space required to hold them. These figures are only guides, as they vary between the software used to produce the documents – generally indicated by the file extension. Many variables, including especially large image and video files and file compression, will affect the actual numbers below.

I have tabulated below an indication of Data Size[74] and/or Electronically Stored Information (ESI) to create a link to the physical size of data.

Name	**Average Pages/ Document**	**Total Pages**	**Capacity**	**Paper Comparison**
CD		50,000	650 MB	20 photocopy boxes of paper
DVD		350,000	4.7 GB	140 photocopy boxes of paper
DLT Tape		3 to 6 Million	40/80 GB	2300 photocopy boxes of paper
Super DLT Tape		4 to 9 Million	60/120 GB	3400 photocopy boxes of paper
Average Page Capacity				
		75	1 MB	
		75,000	1 GB	1000 MB (190 lever arch files)
Typical Software				
Email	1 ½	100,099	1GB	
Word Doc	8	64,782	1GB	
Spreadsheet	50	165,791	1GB	
Power Point	14	17,552	1GB	
PST File (Outlook)		900 emails and 300 attachments	100 MB	
PST File (Outlook)		3,500 emails and 1,200 attachments	400 MB	
NSF Email File		9,000 emails and 3,000 attachments	1.00 GB	

[74] Source e-Discovery Team. http://ralphlosey.wordpress.com

Terms of Size	Equivalent Size	Comment
8 bits	1 byte	one or two words
1,024 bytes	1 kilobyte (KB)	1000 words
1,024 kilobytes (KB)	1 megabyte(MB)	
1,024 megabytes	1 gigabyte (GB	van full of paper
1,024 gigabytes	1 terabyte (TB)	50,000 trees of paper
1,024 terabytes	1 petabyte (PB)	250 Billion pages of text
1,024 petabytes	1 exabytes (EB)	1 000 000 000 000 000 000 words or bytes

4.2. Examples Of What These Figures Mean In Practice

In the case of *Hands v Morrison Construction Services Ltd,*[75] which concerns an application for pre-action disclosure under CPR 31.16, arising out of a claim for breach of representations made by Morrison, in respect of some construction works at Rockingham Speedway. There was a construction adjudication proceeding this application between Rockingham and Morrison about a surface water problem, which led to a decision being given, which found against Morrison on reasonable care and skill, on 18th November 2003. The court considered the detailed implications of the pre-action disclosure but the relevant point for us is that Briggs M, QC summarised the statements made in defence of the application[76] in relation to the size and cost of the task in the event the court granted the order sought. The statistics were given as follows:

- 550 hard copy files search costs estimated at £100,000.
- 1855 gb of data on ten servers which equates to 850,000 lever arch files – cost to upload to a database and carry out a preliminary word search would take 50 days at a cost of £90,000.

In the event the court directed a more limited order, albeit it would appear the parties noted that it would still be a burden, but the court felt it would focus the minds[77].

In the recent patent infringement case of *Nichia Corporation v Argos Ltd,*[78] the Court of Appeal had to consider disclosure of documents in respect of the making of the invention and certain experiments, regarding white LED[79] Christmas lights for which the Claimant alleged there were two patent infringements. Pumfrey J[80] refused both kinds of disclosure at first instance. The case considered proportionality and justice and Jacob LJ equated the cost of disclosure with what the likely damages would be and decided to only allow a restricted disclosure. However, Lord Justice Rix dissenting [81] said that '*a reasonable search should be tailor-made to the value and*

[75] Adj.L.R. 06/16 [2006]; EWHC 2018: c 16th June 2006
[76] Para 49
[77] Para 72
[78] [2007] EWCA Civ 741
[79] Light emitting diodes
[80] [2007] EWHC 545
[81] Para 72

significance of the likely product of such a search' and allowed the appeal and Lord Justice Pill agreed.

Following the consideration of costs in another patent infringement case this time in the US District of California, *Qualcomm Inc v Broadcom Corporation*[82], the Court in respect of a request for sanctions against the Plaintiff's legal team, found that some of 40,000 documents (containing some 300,000 pages) had not been disclosed. In addition, in direct contrast to the statements made in Court 21 emails were found disproving what the Plaintiff had told the Court. Apparently these were not disclosed on the legal team's instruction. The Court was not impressed and as a result the team were directed to participate in a 'Case Review and Enforcement of Discovery Obligations programme (CREDO) and the Plaintiff was to pay the legal costs of the Defendant of some $8.5 million. The statistics are:

- 40,000 documents – 300,000 pages were not disclosed;
- $8,568,633,024 in costs and sanctions;
- he lawyers were reported to Professional Bodies;
- time on CREDO - Case review and enforcement of discovery obligations.

The high profile cases tend to stimulate debate particularly in the US and appear to be closely monitored by other jurisdictions. If we look at Article 3.3 of the IBA Rules of Evidence it states that:

> *'A Request to Produce shall contain:*
> *(a) (i) a description of a requested document sufficient to identify it, or*
> *(ii) a description in sufficient detail (including subject matter) of a narrow and specific requested category of documents that are reasonably believed to exist;*
>
> *(b) a description of how the documents requested are relevant and material to the outcome of the case; and*
>
> *(c) a statement that the documents requested are not in the possession, custody or control of the requesting Party, and of the reason why that Party assumes the documents requested to be in the possession, custody or control of the other Party.'*

This clearly adopts a focused request for specific disclosure but will this resolve the issue of cost by concentrating on the test of relevance? This was reviewed by the New Zealand Law Commission[83] who recognised the need to reduce costs and approved the CPR procedures to make the cost more proportionate. Later in 2006 New Zealand introduced a new Evidence Act[84] to make the admissibility of technology based evidence easier.

[82] [2008] 05cv1958-B
[83] Report 78 – Dealing with Mischief 2002.
[84] s137 provides for the admissibility of evidence produced wholly or in part by machine, device or technical process (for example scanning). s137 says:
(1) If a party offers evidence that was produced wholly or partly by a machine, device, or technical process (for example, scanning) and the machine, device, or technical process is of a kind that

The New Zealand High Court Rules[85] specifically allows a Judge to consider whether a party has impeded the process of discovery and inspection by including documents in an affidavit that are not required to be included and permit the Judge to order the party to pay costs to a party or parties specified in the order[86].

Closer to home in the case of *Abela and others v Hammonds Suddards and Others*[87] the claimant had alleged negligence by the solicitor and misdealings by one partner in particular. Disclosure orders were sought which included the list of Hammonds e-mails and electronic documents, although disclosure was not ordered for personal mobile phone records the cost was recorded at £10. However, disclosure was sought for other telephone records including personal landline and office records and the claimant indicated a willingness to pay the cost of the exercise in any event capped at £10,000[88]. The judge considered that this willingness may be relevant to any question of striking a balance between the particular steps to be taken in electronic disclosure in order to identify disclosable documents although this would not render documents disclosable which would otherwise be inadmissible[89].

The defendant did not serve a list of documents by individual documents but rather by file number and the judge ordered that a separate list should be prepared[90]. As regards electronic documents, the defendants submitted that data on tapes would need to be transferred onto a searchable storage system and that specific hardware and software media would be required which would be operated by senior IT staff. The defendants provided a quotation from its IT department in respect of the recovery of data from backup tapes in the region of £150,000. However, this failed to impress the court[91] who directed ways in which a more useful search might be undertaken[92] and for the defendants to provide a more detailed account of the stored data.[93] It also directed the parties to meet to narrow or, if possible, to resolve the issues[94], pending a further hearing.

---

ordinarily does what a party asserts it to have done, it is presumed that on a particular occasion the machine, device, or technical process did what that party asserts it to have done, in the absence of evidence to the contrary.
(2) If information or other matter is stored in such a way that it cannot be used by the court unless a machine, device, or technical process is used to display, retrieve, produce, or collate it, a party may offer a document that was or purports to have been displayed, retrieved, or collated by use of the machine, device, or technical process.

[85] Schedule 2 High Court Rules, pt 8 Interrogatories, and discovery, and inspection, Subpt 3—Discovery states at r8.18. The default terms of discovery order are: (1) A discovery order is in the terms set out in this Rule unless those terms are modified by the order. (2) Each party must make an affidavit of documents that lists the documents that—(a) are or have been in that party's control; and (b) relate to a matter in question in the proceeding. (3) The affidavit of documents must— (a) comply with rr 8.20 and 8.21; and (b) be filed and served on every other party who has given an address for service. (4) Each party must comply with the order within 20 working days after the date on which the order is made.

[86] Under r8.29

[87] Unreported Lawtel 2009 before Girolami P QC ,Ch Claim No HC07C00250

[88] Para 89

[89] Para 91

[90] Para 113

[91] Para 122 (3)

[92] Para 122 (7)

[93] Para 123

[94] Para 123

4.3. The Storage Process

As a tribunal we have to ask ourselves how much should we really understand about the storage of data? If we, as arbitrators, are being asked to assist the electronic disclosure process then I believe we should have an appreciation of the terms and process being undertaken. The first thing to note is Electronically Stored Information is referred to as 'ESI' and I note that some of the US court decisions have adopted the term without definition.

The other term we hear about is 'metadata', I will now attempt to demystify the process and its terms.

4.4. Metadata

Metadata records data about data elements or attributes, (name, size, data type, etc), data about records or data structures (length, fields, columns, etc) and data about data (where it is located, how it is associated, ownership, etc.).

Metadata may include descriptive information about the context, quality and condition, or characteristics of the data, but much of this is neither created by, nor normally accessible by, the computer user. For example, in a normal word processed document there are hidden codes that determine such features as paragraphing, font, and line spacing. The ability to recall deleted information, normally text, is another familiar function, as is tracking of creation and modification dates.

Similarly, spreadsheets may contain calculations that are not visible in a printed version or hidden columns that can only be viewed by accessing the spreadsheet in its "native" application[95]. Internet documents contain hidden data that allow for the transmission of information between an internet user's computer and the server on which the internet document is located.
You may have heard the term "meta-tags"; these allow search engines to locate websites responsive to specified search criteria, which is why when you use a search engine a vast list of related information is displayed. Whereas "cookies" are text files placed on a computer (sometimes without user knowledge) that can, among other things, track usage and transmit information back to the cookie's originator.

There are two types of metadata. First there is metadata created by the application which travels with the file and secondly, system metadata which, for example, tells the computer where your files are.
So what is important about it? Can the data be relied on? Personally I do not think it is conclusive. If there is more than one person using a PC for example the metadata will not tell you who wrote, edited or printed the documents as the PC cannot tell, as yet, who is pressing the keys after an operator has logged on even with biometric access and passwords. Until this changes, metadata may have only two benefits which are to assist in searching for documents and recording what happened to that document.

[95] The software application used to create or record the information.

Authorship of information can have significant consequences. It was reported[96] in 2003 that the British government released documentation for its case in joining the Iraqi war and this was largely plagiarised from a 13-year-old PhD thesis. Apparently it contained electronic fingerprints of four civil servants who created it and these were within the document when it was released electronically on Number 10's website. It was reported that this metadata showed that instead of the document being prepared by the Foreign Office, it was worked on by civil servants under the control of Alistair Campbell.[97] The paper reported that Mr Campbell apologised for a "mistake" in the dossier, saying "the sole error was for tracts to be culled from a published journal without attribution" when admitting these facts before the Foreign Affairs Select Committee. Apparently the paper is no longer on the website.

Word-processing software includes within a document, the name and size of the font in conjunction with the coded characters themselves, as well as other information, such as the colour of the letters and the colour of the background. This is possible as the underlying text is represented as ASCII [98]codes. However, it remains relatively easy to locate individual letters or substrings, to add or delete text, and to perform other such common text-processing operations. When a user positions a cursor over the letter on the screen, the program knows the location within the file of the character over which the cursor is positioned. Computer software can, in turn, render the character codes as images of characters[99]. Hence it is possible that every action during the life of the document is recorded by metadata.

In a recent civil rights case of *Adraina Aguilar et al v Immigration and Customs Enforcement Division of the Unites States of Department of Homeland Security et al*[100] which was brought by 30 Latino plaintiffs complaining of unlawful searches of their homes, in violation of the Fourth Amendment, the Court had to consider the production of electronic documents because Counsel had failed to discuss the issue early in the case. In the event the Court partly granted the application to compel the production of metadata. The Defendant had to produce the metadata attached to emails, excel spread sheets and powerpoint files and had to provide training sessions to enable the database to be interrogated.

Whilst the metadata can provide proof of authorship, it can if needed, provide the dates and times of an event to support certain propositions. For example I am minded of the need to prove the date and time of receipt of an email for service of documents, which requires a little more effort than checking times of service via facsimile. The cost implication of validating email is thus evident.

[96] According to the Evening Standard of London 25th June 2003.
[97] e-discovery hidden data 0137135599_ch03.pdf
[98] American Standard Code for Information Interchange (ASCII), is a coding standard that can be used for interchanging information, if the information is expressed mainly by the written form of English words. It is implemented as a character-encoding scheme based on the ordering of the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that work with text. Most modern character-encoding schemes—which support many more characters than did the original—have a historical basis in ASCII.
[99] http://en.wikipedia.org/wiki/ASCII
[100] 07 Civ 8224 (JGK)(FM) Filed 21st November 2008.

4.5. Sedona Principles

The problems and costs in the US have led to regular conferences being held to consider electronic documents from which a group of eminent lawyers, academics and jurists have taken part in a project known as The Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production. The Sedona Principles were first published in January 2004 and more recently following developments in the US, they published the Second Edition in 2007.

The following are extracts from the Sedona Principles[101] which you will see are quite extensive:

1. Electronically Stored Information (ESI) is potentially discoverable and organizations must properly preserve ESI that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for ESI, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing ESI, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of ESI when these matters are an issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests for ESI should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

5. The obligation to preserve ESI requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant ESI.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own ESI.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant ESI, were inadequate.

8. The primary source of ESI for production should be active data and information. Resort to disaster recovery backup tapes and other sources of ESI that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the ESI from such sources, including the disruption of business and information management activities.

[101] The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, Second Edn 3-4 (The Sedona Conference® Working Group Series, 2007).

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual ESI.

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of ESI.

11. A responding party may satisfy its good faith obligation to preserve and produce relevant ESI by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data reasonably likely to contain relevant information.

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing ESI should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information may be shared by or shifted to the requesting party.

14. Sanctions, including spoliation[102] findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant ESI, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

4.6. The Basic Process of E-discovery

It is important to first define the collection requirements which will assist the parties in choosing suitable software to analyse the ESI. The chosen software should basically process the data and should;

- Flag up duplicated documents;
- Possibly create threads that run through the documents including any missing messages;
- Carry out keyword and concept searches;
- Code documents in bulk to enable suitable culling or review;
- Group documents into facts or issues;
- Provide ease of use for review.

[102] http://en.wikipedia.org/wiki/Spoliation_of_evidence. In law, spoliation of evidence is the intentional or negligent withholding, hiding, alteration or destruction of evidence relevant to a legal proceeding and is a criminal act in the USA.

The parties should then agree how the documents should be indexed.

In the US there have been several cases which have specified the coding system which they call Bates Numbering. The term is derived from the name of an automatic alpha numeric numbering device. One such case was *USA v Michael John O'Keefe Sr & Sunil Agrawal*[103] where the Court set out that the government should use the following indexing system:

Bates Number	Author	Author's Title	Recipient (if any)	Date of Creation	Location of Document
JEX 1	John Smith	Assistant to the Visa Unit Chief	Betty Brown	2/2/2005	Toronto Consulate / Office of Betty Brown / File Cabinet/ Folder Labeled Expedited Appointment Correspondence

So in summary what can the software do with ESI:

- Files and documents can be imported into databases;
- The details of e-mails including dates and addresses and subject can be imported into a list;
- Everybody refers to metadata and what a wonderful hidden source that is but in reality this seems at present to be very rarely used but in the end, data can be searched, exchanged and filtered to provide reports.

5. Arbitration Practice Procedures

[103] [2008] 06-249 p12

5.1. The Question Is Why Should We As Arbitrators Be Concerned?

Globally the use of 'paperless information' is becoming more acceptable. The European Commission launched an initiative in December 1999 called 'eEurope' which approved and adopted the strapline of 'eEurope - An Information Society For All'[104]. This formed part of the Lisbon[105] Strategy[106] which sets out certain objectives, one of which is '*bringing every citizen, home and school and every business and administration into the digital age and online.*' [107]

Part of its action plan was to stimulate the use of the internet. This framework has recently been revised to the i2010[108] initiative. i2010 is the first initiative taken by the Commission within the renewed Lisbon partnership for growth and employment. This strategy follows on from two action plans, eEurope 2002 and eEurope 2005, which set out the steps to be taken to promote Information and Communication Technologies (ICT) in Europe.

i2010 centres on three priorities[109]:

- completing a single European information space which will encourage an open, competitive internal market for the information and media society;
- promoting innovation and investment in research into information and communication technologies (ICT);
- creating a European information society based on inclusion and stressing better public services and quality of life.

The expansion of technology into more homes, businesses and government increases concerns over data retention, privacy and confidentiality issues. In addition you really do not know who is holding, or has access to your data and where it is within the world of servers. Thus in regard to both domestic and international disputes it is more than likely that the consideration of requests for disclosure will be become more regular and complex and may include cross border jurisdictional issues.

5.2. Arbitration Act 1996

I will now look at the process in respect of arbitration but I will start with some extracts from the widely adopted UNCITRAL Model Law[110].

[104] http://ec.europa.eu/information_society/eeurope/2002/index_en.htm
[105] Lisbon Treaty http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML
[106] Lisbon Strategy http://europa.eu/scadplus/glossary/lisbon_strategy_en.htm
[107] http://europa.eu/scadplus/glossary/eeurope_en.htm
[108] http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm
[109] http://europa.eu/scadplus/glossary/infoso_media_policy_guidelines_en.htm
[110] United Nations Commission on International Trade Law Model Law on International Commercial Arbitration as adopted 21st June 1985.

The Model Law under Article 18 says:

> *'the claimant may annex to his statement of claim all documents he deems relevant or may add a reference to the documents or other evidence he will submit.'*[111]

The Model Law helpfully says that each party shall have the burden of proving the facts relied on to support his claim or defence[112] and that any time during the arbitral proceedings, the arbitral tribunal may require the parties to produce documents or exhibits or other evidence within such a period of time as the tribunal shall determine[113].

The English Arbitration Act 1996, was based on the Model Law. Section 34 subsection 2d of the Act provides that the arbitrator may decide:

> '*Whether any and if so which documents or classes of documents should be disclosed between and produced by the parties and at what stage.*'

This is an extremely wide power but is only really subject to protection against the disclosure of privilege documents or any contrary agreement between the parties and the overriding obligation in Section 33 of the Act. This requires the arbitrator to:

a) '*act fairly and impartially as between the parties giving each party a reasonable opportunity of putting its case and dealing with that of his opponent*'.

b) ' *adopt procedures suitable to the circumstances of the particular case, avoiding unnecessary delay or expense as to provide a fair means for the resolution of the matters falling to be determined*'.

If the power afforded under s33 & 24d are used correctly arbitrators should be able to prevent expensive disclosure and exercise control over the production of documents.

However, the arbitrator should apply the principles of relevance and necessity to ensure effective disclosure orders are made without, hopefully, any abuse of the process which can occasionally occur. The application of common sense may also assist in the decision-making process, being mindful of s33 obligations to promote a fair and expeditious resolution of the dispute on a cost-effective basis.

In construction there are some interesting arguments regarding which documents are in the possession of a party. For example, all documents held by an employee are clearly in his possession. If documents are in possession of an agent i.e. an architect, they may be within the power of the party if they emanate from him or obtained by the agent on his behalf. The distinction here is if the documents came from the agent, for example, his working papers, these are not in possession or power of the party and

[111] A similar provision is made for the defence albeit the wording is slightly different insofar as the respondent may annex to his statement the documents on which he relies for his defence.
[112] Art 24.1
[113] Art 24.3

he cannot be compelled to disclose them. However it may be that the party who wishes to use the documents will have to prepare a witness summons and issue it under the relevant court proceedings. In the UK CPR Rule 34.2, the arbitrator has no inherent power to apply for a summons but permission can be granted to an applicant party by the arbitrator under Section 43 of 1996 Act.

Construction cases often produce considerable volumes of paper and it is therefore important to identify all categories of documents which are to be disclosed through the pleading process and indeed those which will be used at the hearing. It may be appropriate to warn that the cost of disclosure be recorded separately by each party to assist in the assessment costs at the end of the hearing. Indeed it may be an appropriate point to discuss the capping of costs for disclosure[114]. However, in my experience every time I have referred the parties to this provision they declined the opportunity to have any form of limit. Also I think it is difficult to impose a limit early on in the process because the full extent of the issues to be decided is not always known. In this event it may practical to set limits for particular stages of the process.

Section 34 (2) (f) of the 1996 Act allows the tribunal to decide:

> "*Whether to apply strict rules of evidence (or any other rules) as to the admissibility, relevance or weight of any material (oral, written or other) sought to be tendered on any matter of fact or opinion and the time manner and form in which such material should be exchanged and presented*".

In order to operate the power under Section 34 (2) (f) there are various factors that need to be considered:

1. Relevance - the evidence should be relevant to the issue in order to logically prove that matter in issue;

2. Is the information privilege and if so should it be excluded?

3. When deciding an issue the arbitrator should ensure that when he makes a finding of fact, it is supported by the evidence produced and he must consider the way that evidence is provided. In other words the award must be on a sure foundation of fact.[115]

Mustill and Boyd[116] identify the point that the Civil Procedure Rules are a codified system with its own policy and spirit. Nevertheless, it concludes that the tribunal may think it useful to consider an order for standard discovery whereby the party is required initially to disclose only the documents, on which it relies, or those which adversely affect his own case and those which support its opponent's case[117]. Alternatively, the tribunal may wish to order that each party after the first round of disclosure has taken place, is entitled to call for production of specific documents or

[114] s65 of The UK Arbitration Act 1996.
[115] Air Canada and Others v The Secretary of State for Trade and Another (No 2) [1983] 1 All ER 61 as per Bingham J
[116] Commercial Arbitration by Lord Mustill and Stewart Boyd 2nd edn 2001 Companion p 191
[117] r 31.6

classes of documents, and by suggesting this it recognises the arbitrator has a very wide power.

Therefore, it is apparent that there are similarities between the Arbitration Act 1996 which is based on the Model Law, and the CPR.

Often arbitrators will be asked to order standard disclosure by legal advocates. The term Standard Disclosure is defined in CPR 31.6 which requires a party to disclose only the documents on which it relies, and the documents which adversely affects its own case or affects another party's case or supports another party's case. But let us look how various UK and some International Arbitration Rules handle disclosure.

5.3. UK Rules

CIARB

In the Chartered Institute of Arbitrators Arbitration Rules[118] Article 8.4 allows parties to include with any pleading, a copy of any document which they consider necessary to their claim. Also Article 8.7 says, in respect of procedure, that before or after close of pleadings the arbitrator may give detailed directions including disclosure and production of documents as between the parties.

Further, under the first schedule which is the Short Form Procedure for document only cases, Article 8 is replaced by paragraph 2. This states at clause 2.3 that the statement of case shall include[119] copies of all documents, the contents of which the party relies upon and at clause 2.5 the provisions of Article 8.7 (B) are restated.

CIMAR

Under the Construction Industry Model Arbitration Rules[120] the arbitrator shall determine which documents or classes of documents should be disclosed between and produced by the parties and at what stage[121] . It is apparent that whilst there is a definition of terms at Appendix 1 to the Rules, 'documents' have not been defined.

ICE

The Institute of Civil Engineers requires the statement of case to include a list and/or summary of the documents relied upon[122]. Also the rules allow the arbitrator to determine which documents or classes should be disclosed[123].

[118] 2000
[119] [2.3(iii)]
[120] Rules drafted by the Society of Construction Arbitrators in consultation with the construction industry and other professional bodies, referred to as CIMAR 1998.
[121] r5.2
[122] ICE Arbitration Procedure 1997, r8.1
[123] ICE Arbitration Procedure 1997, r8.2

LMAA

By comparison, although the London Maritime Arbitrators Association Small Claims Procedure[124] refers to the disclosure of documents, there is no discovery in this Procedure. Except that, if in the opinion of the arbitrator a party has failed to produce any relevant documents, he may order the production of the document and may indicate to the party to whom the order is directed that, if without adequate explanation he fails to produce a document, the arbitrator may proceed on the assumption that the contents of the document do not favour that party's case.

Helpfully these Rules[125] define the expression relevant document which it says 'includes all documents relevant to the dispute whether or not favourable to the party holding but it does not include documents which are not legally disclosable'.

LCIA

The London Court Of International Arbitration Rules says:

> "all statements and that means written submissions referred to in this article shall be accompanied by copies (or, if they are used specially voluminous, lists) of all essential documents on which the party concerned relies and which have not previously been submitted by any party and (where appropriate) any relevant samples and exhibits."[126]

But under Article 22.1 (B) there is a non-mandatory provision to give the arbitral tribunal the power to order any party to produce to the arbitral tribunal, and to the other parties for inspection, and to supply copies of, any documents or classes of documents in their possession, custody or power which the arbitral tribunal determines to be relevant.

5.4. International Rules

Hong Kong

This theme is repeated in the Hong Kong International Centre Domestic Arbitration Rules,[127] which say that the arbitrator has power to order any party to produce to the arbitrator and to supply copies of any documents or classes of documents in their possession, custody or power which the arbitrator determines to be relevant[128].

Sweden

Under the Arbitration Institute of the Stockholm Chamber of Commerce, rules for Expedited Arbitration say:

[124] 2002 r6
[125] Rule 6B
[126] 1998 art 15.6
[127] 1993
[128] Art 11 (D)

"at the request of the arbitrator the parties shall state the evidence on which they intend to rely, specifying what they intend to prove with each item of evidence and shall present documentary evidence on which they rely. Subclause (2) says the arbitrator may refuse to accept evidence submitted to him if such evidence is considered to be irrelevant, non-essential or if proof can be established by other means which the arbitrator considers more convenient or less expensive."[129]

These Rules provide an interesting addition to the Arbitration Rules because it provides the arbitrator with more power over case management which has been a recent criticism of the rising costs in litigation.[130]

Canada

The National Commercial Arbitration Act of Canada 2004 relies on the Model Law. Article 23 (1) of which provides that:

> *"the claimant shall state the facts supporting his claim, the point at issue and the relief already sought and the respondent shall state his defence in respect of these particulars unless the parties have otherwise agreed as to the required elements of such statements. The parties may submit with their statements all documents they consider to be relevant or may add a reference to the documents or other evidence they will submit.*"

New Zealand

The New Zealand Arbitration Act 1996 and 2007 amendments are based on the Model Law, as are some other Arbitration Acts, but it is apparent from the above examples that the principles of relevancy is paramount in deciding the document to disclose.

The International Institute for Conflict Prevention and Resolution

The Institute produced some rules for expedited arbitration of construction disputes in June 2006. These rules are interesting in so far as in respect of discovery, Rule 11.2 states that:

> *"the tribunal may require and facilitate such other discovery as it determines is appropriate in the circumstances, taking into account the needs of the parties and the desirability of making discovery expeditious and cost-effective. Electronic discovery will not ordinarily be permitted except in the discretion of the tribunal…"*

This is the only set of arbitral rules I have found which specifically refers to electronic disclosure. In addition, the introduction to these rules highlights that the period between the prehearing conference and the commencement of the hearing is set at 100 days[131], which includes 60 days for discovery.

[129] 1999 Art 22
[130] See supra para 2.4
[131] As set out in rule 1.3

5.5. Chartered Institute of Arbitrators Protocol For E- Disclosure

The Chartered Institute of Arbitrators recently released a protocol for potentially disclosable documents in electronic form to achieve an early consideration of those documents to avoid unnecessary cost and delay and in a format which allows parties to adopt the protocol as part of the agreement to arbitrate. I have provided everybody with a copy of this protocol for you to read as appropriate but you will note that it covers some of the issues I have referred to in this paper. Therefore, I have no hesitation in recommending it to you as a workable document which can be applicable in other jurisdictions.

5.6. Techniques for Controlling Time and Costs in Arbitration

A report from the ICC Commission on Arbitration[132] recorded that costs of arbitral proceedings for 2003 and 2004 were on average divided as follows:

Costs borne by the parties to present their case	82%
Arbitrators fees and expenses	16%
Administrative Cost of the ICC	2%

With these figures in mind the ICC set about producing guidelines on how to minimise the costs by good management, having regard to the parties' rights to put forward their case.

The guidelines suggest that the parties should consider avoiding requesting documents that are not relevant and material to the outcome of the case, and documents that are not needed to prove agreed facts[133].

It is sensible to establish a procedure for production of documents as this can effect time and costs savings. In doing so the guidance notes refer to the use of the IBA Rules of Evidence and to agreeing a clear and efficient system. Also it suggests[134] that the costs can be further reduced by agreement on:

1. Limiting the number of requests;
2. Limiting requests to documents (whether in paper or electronic form) that are relevant and material to the case;
3. Establishing reasonable time limits for the production of documents;
4. Using the Alan Redfern Schedule which follows the lines of a Scott Schedule.

Identify Document or Category of Documents	Reasons for Request	Summary of Objection for Disclosure of Document or Category	Arbitral Decision

[132] ICC Publication 843 - Techniques for Controlling Time and Costs in Arbitration, Introduction, p6, published by the ICC 2007 http://www.iccwbo.org/uploadedFiles/TimeCost_E.pdf
[133] Para 53
[134] Para 55

It also comments[135] about the common problem of duplication of documents in the statement of case, statements and other submissions, and issuing the tribunal with every document[136]. It confirms that doing this increases costs and makes it more difficult for the tribunal to prepare, so it suggests that only a selection which is material to the determination of the case is provided. It also recognises the use of electronic transfer of documents[137] as a means of saving costs.

5.7. Conclusion

The competent discovery of all relevant documents in a proceeding involves the application of the appropriate rules but more importantly common sense. The discovery process highlights the necessity of clear and well thought out pleadings to ensure all of the issues are raised at an early stage and to ensure discovery is completed in a timely and cost effective manner. Poor pleadings will let a party down at the discovery stage as all of the issues may not be identified and the party will be put through further, possibly unnecessary expense, in amending pleadings and making application for further discovery. This in itself will lead to further cost issues.

The arbitrator must therefore be on his guard to ensure that the party is aware that an unrealistic discovery request may mean a substantial cost burden for him[138]. There seems to me to be no reason why an order should be given for security of those costs.

Sensible use of IT will also have a cost benefit, so moving on in the 21st Century, how can arbitration benefit from technology?

[135] Para 56
[136] Para 57
[137] Para 58
[138] Access to Justice 1995, Lord Woolfe stated 'the benefits of a system of discovery will only outweigh the disadvantages if substantially greater control over the scale of discovery is exercised than at present'.

6. Data Management

6.1. Technology

I have already mentioned ESI, MB and GB, but there is often some confusion between 'bit' and 'byte' that is apart from terms such as IP, ISP, LAN, WAN, TCP/IP, iSCSI. It is not within the scope of this paper to provide a full glossary of terms but I will give a brief explanation of the common terms we are likely to be faced with.

A bit[139] comes from the phrase 'Binary digIT'. It is the smallest unit of computer data whereas 'byte' is eight bits. This is why there is some confusion when data streams are measured in bits/second and memory or hard drives are quoted in bytes.

ESI is stored information, which is held on media of some sort. The quantity is measured in MB or GB in a language. That language can, for example, be in DOS, Novell, Linux, ASCII or Mac OS. If it is a database it can in Visual Basic, C++, Oracle and others. Unfortunately the software industry only supports old software versions for a limited period of time and so it is not always possible to recover or read old data with current software. If it is recoverable then some of the functionality of the original document may not survive the process and so the representation of the original may be different. However, the same problems can occur with hardware, being largely mechanical, the systems sometimes fail and direct replacements may not be available.

Each computer in the world has a unique ID. Often it is called an IP address – Internet Protocol. When computers are linked in a network they recognise each other by their TCP/IP address where TCP means Transfer Control Protocol. If the computers are linked in an office it is called a Local Area Network (LAN). If there are networks connected from outside it is a Wide Area Network (WAN), which if global is WWAN[140]

To give you an idea of how a WAN appears I have a picture of the Perdue University computer network[141] in Indiana, USA that is still developing and as you can see illustrates the need for careful planning and careful management.

The increased use of the internet has led to new technologies such as the development by the Internet Engineering Task Force (IETF)[142] of the Internet Small Computer System Interface (iSCSI). This is an Internet Protocol based storage networking standard for linking data storage facilities[143].

[139] Is a single digit number to the base-2 in binary code.
[140] World Wide Area Network.
[141] Network Maps Perdue University in Indiana.doc
[142] The Internet Engineering Task Force (http://www.ietf.org/index.html) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
[143] By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. The iSCSI protocol is among the key technologies expected to help bring about rapid development of the storage area network (SAN) market, by increasing the capabilities and performance of storage data transmission. Because of the ubiquity of IP

So the development continues, but what are the main forms of ESI we will encounter?

- Memory cards
- Hard drives in PC and portable devices
- Network Accessed Storage
- Tapes
- DVD/CD
- USB
- Phone cards
- PDA/Blackberry
- Digital voice recorders – used for quality purposes
- Voice Mail systems and other telephone recording devices
- Webmail
- Photocopiers and printers with hard drives
- GPS devices
- Video cameras with memory cards and hard drives.

I will show you some examples and the internal workings of a hard drive and disk. (A practical demonstration was given.)

6.2. The Size of the Problem

In August 2008, a Web-based survey by TechRepublic[144] members[145] was carried out to better understand how companies are supporting e-discovery. The survey showed some startling statistics.

The members were advised that 'when electronically stored information (ESI) is subject to discovery, it is referred to as e-discovery, and it must be located, secured, and searched for use as evidence in a trial.' And in response to various questions, the survey results showed that 22% had been involved in e-discovery in the last five years and that the main cause was contractual disputes. Despite this only 30% of companies reported in the survey that they had any training in ESI or e-discovery.

This survey was carried out world wide and shows a wide lack of understanding for the problems of ESI. So let's look at some data issues within the UK.

networks, iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval.

[144] Source: TechRepublic an online resource for IT professionals E-Discovery Survey, August 2008 http://techrepublic.com.com/

[145] 711 no.

6.3. Recorded Information and Email

The need to take proper corporate control of data is further highlighted by:

6.3.1. Freedom of Information Act

The Freedom of Information Act 2000 ("FOIA")[146] which came into force on 1st January 2005 and gave the public new rights of access to recorded information held by public authorities. Email communications fall within the definition of "recorded information". Anyone, anywhere, without giving either proof of identity or details of their motive for making a request, can ask for a copy of an email and the authority has to respond within 20 working days from the date of receipt of the request. Clearly many have failed as can been seen from the Information Commissioner's website.[147]

However, s46 of the FOICA requires the authority to comply with a statutory code on record management which needs to be part of the 'corporate programme'.[148]

In August 2008 the Commission published a practical guidance on redacting and extracting information for local authorities[149] to help them understand their obligations and to promote good practice.

6.3.2. The Data Protection Act

The Freedom of Information Act has revolutionised the public sector's approach to the management and storage of electronic mail but we must not forget the Data Protection Act 1998 ("DPA") which applies to the private and public sector alike. However, although the intricacies of the DPA are outside the scope of this paper we need to briefly look at personal data.

6.3.3. What is Personal Data?

Guidance on the definition of personal data has been provided by the EC Article 29 working party[150] which has attempted to summarise the common understanding of the concept of personal data amongst EU member states. Its opinion, published in June 2007, analyses the 4 main elements of personal data which it says is:

> 'any information relating to an identified or identifiable natural person.'

This definition provides the basis for interpretation of the EC Data Protection Directive (95/46/EEC)[151] by data controllers and national data protection authorities.

---

[146] Received Royal Assent on 30th November 2000
[147] www.informationcommissioner.gov.uk
[148] Latest guidance from 1st January 2009.
http://www.ico.gov.uk/what_we_cover/freedom_of_information/publication_schemes.aspx
[149] 22nd August 2008 Version 1
http://www.ico.gov.uk/upload/documents/library/freedom_of_information/practical_application/redactingandextractinginformation.pdf
[150] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm
[151] http://www.cdt.org/privacy/eudirective/EU_Directive_.html

DPA also requires organisations to take appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data against accidental loss or destruction. This means that access to any e-mail system and related storage devices should be controlled whether that access is internally or externally to the organisation. Any sensitive personal data needs to be treated with special care, and so a secure archive is likely to be helpful and provide an essential backup should there be a failure of the main system.

6.3.4. The Evidential Email Burden

In the recent case of *Digicel (St Lucy) Limited and Others v Cable and Wireless Plc and Others*[152], the court had to consider what constituted a reasonable search for and in electronic documents. In that case it held that the defendants had not carried out a reasonable search "insofar as they had omitted to search for and in the specified e-mail accounts to the extent that those e-mail accounts might exist in the backup tapes which had survived".

The ability to archive and retrieve data may have an effect on the weight that can be attached to the evidence. Favourable evidence is based on the reliability of that evidence, and on that basis any evidence obtained from an insecure and unreliable system which is not particularly well governed or clearly documented may be open to dispute and questioning by the opponent. Therefore, it follows that any organisation that can demonstrate that the e-mail evidence has been created, compiled, stored and retrieved in accordance with good industry practice, is more likely to enhance the reliability of their evidence.

The British Standards Institution Code of Practice for legal admissibility and evidential weight of information stored electronically was published in 2003.[153] It provides a framework that is aimed to assess the reliability of evidence from ESI. Obviously compliance with this Code does not automatically ensure that any documents are reliable but it would strengthen any arguments over authenticity. Conversely failure to adopt the Code may leave an organisation open to suggestion that their evidence lacks any integrity but the BSI also provides guidelines on Records Management for Information and Documentation[154].

Therefore, if an organisation fails to adopt the best possible archiving system and procedures it could mean the difference between winning and losing a case whilst having a significant impact on the cost of the proceedings.

A CPR working party on electronic disclosure, chaired by Mr. Justice Cresswell in 2004[155], noted that:

---

[152] [2008] EWHC 2522 (CH)

[153] Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence': the BSI code of practice, PD 5000:1999, enables organisations to demonstrate the authenticity of their electronic documents and e-commerce transactions, so they can be used as legally admissible evidence

[154] PD ISO/TR 15489-2:2001 BS ISO 15489-2:2001 http://shop.bsigroup.com/ProductDetail/?pid=000000000030048103

[155] Working Party Report para 3.25: http://www.hmcourts-service.gov.uk/ docs/ electronic_ disclosure 1004.doc

> *"at the conclusion of the trial (or earlier if appropriate) judges should give separate consideration as to the costs incurred in relation to e disclosure and who should pay those costs, having regard to the reasonableness and proportionality of the disclosure requested and given, the relevance of the disclosure given or ordered to be given to the issues in the case presented at trial and the conduct of the parties generally in relation to disclosure*".

In order to manage this risk there are several practical steps that can be adopted by any organisation and can include as part of its corporate governance:

1. Using a system that can manage e-mails in line with good industry practice to enhance the reliability of e-mail evidence;

2. Have an internal procedures in place to control the use of e-mail in order to avoid damaging disclosures;

3. Understanding the legal rules which may allow the limited disclosure of e-mails to the other party.

6.3.5. When is an Email Notice Served?

I could not leave the importance of emails without looking at service by email in Arbitration.

The Courts have recognised that electronic documents and communications are normal for most businesses and the rules for disclosure of evidence in court now include electronic documents such as emails. But service by email has not been recognised as effective under the Civil Procedure Rules except in closely defined conditions as set out in CPR 6.2 Practice Direction Paragraph 3.2.[156] This states that service by email is not allowed unless there has been express written willingness to accept email service and the email address has been stated.

It is only when an email address appears on a statement of case or a response to a claim that the address can, of itself, be taken as a sufficient indication to accept legal communication to the email address. However, the Arbitration Act of 1996[157] allows notice to be served by any effective means and the Housing Grants, Construction Regeneration Act 1996[158] has a similar provision.

The question of whether an arbitration can be validly commenced by notice via email was decided in the case of *Bernuth Lines v High Seas Shipping Ltd (The "Eastern Navigator").* [159] The way that Bernuth used the internet and emails was similar to most construction firms. It had a website upon which a 'further information' email address appeared, followed by the postal address and fax and telephone numbers.

[156] http://www.justice.gov.uk/civil/procrules_fin/contents/practice_directions/pd_part05b.htm
[157] s76
[158] s115
[159] [2005] EWHC 3020 QBD (Com Ct) (Christopher Clarke J) - 21 December 2005

Bernuth chartered the ship Eastern Navigator from High Seas but a dispute arose between the two companies.

In May 2005 lawyers for High Seas sent an email giving notice to agree the appointment of an arbitrator. The email address had not appeared on any previous communications. Although Bernuth only intended the 'info' email address to be used for cargo bookings relating to its liner service, there was no indication on the website that it was only to be used for that purpose so in fact the email from High Seas' lawyer arrived at Bernuth's customer services department. It appears that this department received hundreds of spam emails every day, many of them containing apparently legitimate legal correspondence that in fact was spurious.

Nobody at Bernuth expected any serious legal correspondence to arrive via this address so Bernuth's Customer Services department ignored the email with the Notice of Arbitration, but the email generated a 'confirmation of delivery' receipt that bounced back to the lawyers for High Seas.

The arbitration proceedings got under way with both the lawyer for High Seas and the arbitrator sending documents to Bernuth's 'info' email address. Confirmation of delivery receipts continued to be generated and the arbitrator was satisfied that Bernuth was aware of the arbitration proceedings. However, Bernuth was unaware of what was going on until the end of July, when the arbitrator issued his award. He sent it both to the info address and by post and it was by this latter communication that Bernuth first heard of the arbitration, but unsurprisingly the arbitrator held that High Seas was entitled to payment from Bernuth.

Bernuth said that the arbitration was not properly brought to its attention and that there had been a serious irregularity affecting the proceedings that had caused substantial injustice and so it applied to set aside the award under Section 68 of the Arbitration Act 1996.

In court the judge, Mr Justice Clarke, said arbitrations are usually conducted by businessmen represented by, or with ready access to, lawyers and held that the notice provisions in the Arbitration Act 1996 were deliberately wide. As email was a method habitually used by businessmen and lawyers to deliver documents there was no reason to treat email differently from any other form of communication. However, Judge Clarke did add that clicking the 'send' icon did not automatically amount to good service. The email had to be sent to a valid email address of the intended recipient and it must not be rejected.

If the sender did not require confirmation of receipt he might not be able to show that receipt has occurred and where there were several email addresses for different divisions of the same company, sending to a particular email address might not be effective service. But in this case there were none of those difficulties. The emails were all received at the 'info' email address. Moreover, the first email was sent marked with 'High Importance' and all the emails were plain and straightforward and bore none of the hallmarks of spam. Accordingly, Mr Justice Clarke held that if the emails never reached the relevant managerial and legal staff, that was an internal failing and so he declined to set aside the award.

This was instructive case from which the lessons are clear:

- State on your website whether service will be accepted by email.
- Make clear whether an email address can be used to commence legal proceedings.
- Make sure spam filters do not dump legal notices.
- Automatic receipts should state whether the email address is a valid address for service for legal proceedings.
- In construction, many of these matters can be regulated by the underlying contract, but care must be taken not to waive these requirements.
- Adjudicators and arbitrators can assist by ensuring that the first communications are sent to post and fax addresses.

6.3.6. So What Of Signing An E-Mail?

In the recent case of *Mehta v Pereira Fernandes SA*[160] which concerned a promise to pay which was conveyed in an e-mail that was undersigned unlike previous e-mails, the respondent unsuccessfully argued that the automatic insertion of the e-mail address of the sender was a signature for the purposes of the Statue of Frauds[161].

The facts of the case are quite simple in that Mr. Mehta failed to pay the supplier of bedding products and thus the respondent presented a petition to wind up the company. Mr. Mehta asked an employee to send an e-mail to the respondent's solicitors on his behalf asking for the petition to be adjourned and saying that he would give a personal guarantee. This was accepted but he failed to pay and proceedings were commenced under Section 4 of the Statue of Frauds. This stated that no action shall be brought to charge the defendant upon any special promise to answer the date unless the agreement or note shall be in writing and signed by the party charged. Under this section if it is not complied with any agreement is unenforceable.

The court found that an e-mail with just an e-mail address in the 'from' field which is generally automatically completed by your computer will not constitute a signature in itself. It is therefore possible that if you had a completion text which appears automatically at the end of the e-mail identifying the sender with contact details it may not be a signature. However, the case also looked at the Electronic Communications Act 2000 which at section 7 (2) states that:

> '*for the purposes of this section an electronic signature is so much of anything in electric form as:*
>
> > *(A) is incorporated into or otherwise logically associated with any electronic communication or electronic data and,*

[160] [2006] EWHC 813 (CH)
[161] 1677

> *(B) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.*'

The Electronic Signatures Regulations 2002 distinguishes between an '*electronic signature*' which is data in electronic form which is attached and serves as a method of authentication and '*advanced electronic signatures*' which are digital signatures. The latter are admissible in evidence but a signature line that just contains a simple name without any form of independent verification is not admissible in itself.

Therefore, if you receive an e-mail completed along the lines of 'Kind Regards, John' this may create a presumption which may bind the sender. However, it is more than likely that the more important factor is that the sender should have his or her job title properly specified if indeed it is company procedure to state it.

This example above shows that if an employee does not know what they are agreeing to in the e-mail this could potentially lead to disciplinary proceedings or a liability issue for the company. Therefore, it is important that businesses should be careful how employees represent themselves so that they do not appear to have a higher level of authority than they actually do. Hence, be aware that if you use your full name to verify communication it will probably be a valid signature and thus binding.

Whilst this particular point does not necessarily concern the subject matter of the paper I considered it was relevant if we are considering the authenticity and effect of e-mails and management policies in regard to their use and storage.

6.3.7. Guidelines On Email Policy Development

Whilst on the subject of email retention policies, The Sedona Conference 2007[162] developed some useful guidelines to assist with email management policies which should assist in formulating such management strategies. The guidelines are:

"*Guideline 1: Email retention policies should reflect the input of functional and business units through a team approach and should include the entire organization including any operations outside the United States.*

Guideline 2: The team should develop a current understanding of email retention policies and practices actually in use within the entity.

Guideline 3: An entity should select features for updates and revisions of email retention policy with the understanding that a variety of possible approaches reflecting size, complexity and policy priorities are possible.

Guideline 4: Any technical solutions should meet the functional requirements identified as part of policy development and should be carefully integrated into existing systems."

[162] 2007 The Sedona Conference Journal 239
http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110

However, before one looks to formulating such policies an appreciation of data storage would be helpful as each company or entity has evolved its only preferred routine and/or system.

6.4. Data Management Protocol

Backups are taken as a means of disaster recovery but for many, performing the backups is a pointless and boring task. It must be remembered that a hard drive is simply a mechanical device which can fail and although it may be covered by warranty, if it does fail all the documentation may be lost and that part is usually not part of the warranty. It is therefore important to develop a scheduled backup routine to protect your vital data.

Not everybody needs to do a backup everyday. For example, in deciding on your requirements, you need to consider how serious it would be to lose a day's worth of changes in your documents, or in a week or a month? You may be able to get into the habit of running your backups each morning while you are making coffee. Alternatively if the computer is left running overnight the backup routine could run in this idle period. Whatever you decide to do you need to find a time when the data you are backing up is not being accessed. However, many of the backup methods skip the files that are not in use although you can usually guarantee that the missed file is the one you need.

The best practice is to automate the process. The computer can be backed up to several different types of media, some of which I have already mentioned. If you recall in its infancy computers were backed up to diskettes which was a lengthy process as the disks had to be changed. The more advanced systems use fully automated tape rotational devices. The golden rule is that if you suspect a potential hard drive failure, back it up completely by a reliable means and change the hard drive because in reality you never know when it will completely seize or fail to read the data.

Having decided on your backup sequence you then need to decide on how many times you will reuse the media because over a period of time it will deteriorate and when you need it most it will ultimately fail. Hence if you have a particular concern over your data you could take a special backup at say, every month or every quarter. If you use a tape drive, some tapes claim that you can use them 100,000 times but to be certain it is a better policy to have at least 3 backup sets because having one is about as good as having none at all.

How do we protect the backup? In the case of a larger company, backups are usually password protected but they need to make provision for the possibility that the employee who is responsible for the backup process, leaves. Accordingly it should be part of policy that password is known to the subsequent manager so that the backups can be accessed. This may seem a simple requirement but I have heard of several cases typically in the larger firms where this has created a serious problem. In addition, where there was perhaps a lack of care the previous manager did not look at key backup log files to check everything was working as it should and when a

company came to use the backup files, no data had been recorded. If the company had a verification policy it is likely this problem would not have occurred.

When looking at the backup logs there are some shortcuts to help ensure the integrity of your data. For example, you can look at the time taken to run the backup or the number of files you expected or the directories. You may find that there are access problems with some of the servers or PCs around the office which you will need to rectify in order to provide an adequate controlled backup system.

Best practices to testing backups:

- test the backup media from your regular backups;
- ensure you can restore entire directories servers or applications;
- do a test restore to a different computer or server;
- if costs permit have a second tape drive in another location of the same model in case you need one in a hurry;
- make sure you keep a copy of the installation disks for your backup software with your backup tapes or media;
- make sure the procedure for restoring and installing applications is properly documented and as an added precaution included in a text file with the application which is backed up every time;
- keep track and update the backup directories as the organisation develops and/or the file structures change;
- ensure the backup policy takes into account any particular requirements of any applications particularly databases which store files in multiple directories;
- keep a comprehensive note of the backup strategy, file locations, passwords, inventory and in the case of IP addresses, you need to remember that if they are automatically assigned they may change.

Backups can be stored by Directly Attached Storage (DAS) devices which are generally provided to a budget and for which IT managers are generally seeking enhancements because of the increased space requirements. These systems, usually a tape drive, are generally attached to a server and provide a fast backup facility. But if the storage device is not attached or built-in how does that connect to the server?

In all networks there is a server which assigns all connected PC's with an IP address using the Dynamic Host Configuration Protocol (DHCP). This is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual intervention. However, it sometimes transpires that the server for whatever reason reassigns IP addresses and in which case your backup route may be lost. In our office this tends to manifest itself when we are unable to print to certain printers which then have to be manually configured with a new IP address.

If the storage device is attached to the network, it is referred to as network attached storage (NAS). This provides storage on the network which can be accessed by a number of users and can currently store up to 200 TB. The advantage for a smaller organisation is that NAS devices can be linked together as the organisation expands.

The next level is Storage Area Networks (SAN). These are the most expensive particularly if you use fibre channel cabling which requires more expensive equipment. If you wanted to run a SAN system you could do it using the Internet small computer system interface, to which I referred to earlier. Whilst this is beyond the scope of this paper it would require you to have a separate server running on a separate network to ensure security and reduce the amount of traffic on the main network. For those who are interested, Microsoft provide such an initiator in both its 32-bit and 64-bit Windows systems.

A review of data management would not be complete without reference to the Sarbanes-Oxley Act,[163] also known as the Public Company Accounting Reform and Investor Protection Act in the USA which specifically relates to document retention. It was introduced by President George W. Bush in reaction to financial scandals such as Enron and Worldcom. It provides amongst other things that:

- a failure to maintain, audit or review work papers for at least 5 years is punishable by up to 5 years in prison and or a fine;
- corruptly ordering, destroying, or conceding records or documents in order to compromise the integrity of the record for use in an official proceeding is punishable by up to 20 years in prison and/or an unspecified fine amount;
- the alteration, destruction, or concealment of any records with the intent of obstructing a federal investigation carries an unspecified fine amount and/or jail time of up to 10 years.

Hopefully this form of legislation will only be restricted to certain areas but if it is adopted by other jurisdictions then it could be that the task of data retention will develop into a self sustaining industry.

[163] http://www.soxlaw.com/ The Sarbanes-Oxley Act of 2002 (Pub.L. 107-204, 116 Stat. 745, enacted July 30, 2002), and commonly called Sarbanes-Oxley, Sarbox or SOX, is a United States Federal Law enacted on July 30, 2002, as a reaction to a number of major corporate and accounting scandals including Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. These cases cost investors billions of dollars when the share prices and thus the companies collapsed. The act was unanimously approved by the Senate and was named after its sponsors U.S. Sen Paul Sarbanes (D-MD) and U.S. Rep. Michael G. Oxley (R-OH). The legislation sets new and/or enhanced standards for all U.S. public company boards, management and public accounting firms but it does not apply to private companies.

7. Data Recovery

7.1. Practical Demonstration

Let us see if we can recover some data from this hard drive which appears blank, by using this software. The disk has been deleted and re-formatted.

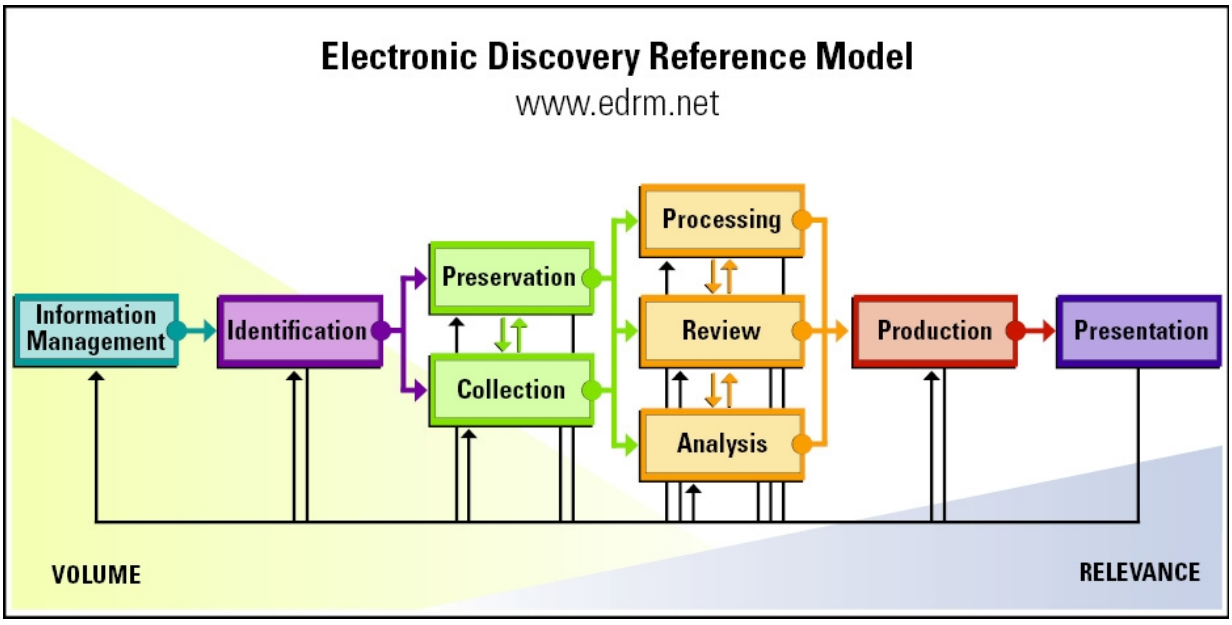
One of the reasons we now see files is that they are like ghosts on the machine. The files are all indexed so the indexing should be linked and the program re-establishes those links.

7.2. Counter Forensic Tools

How do we stop this recovery? Simply either use software that says it can nuke the drive – that is make it unreadable or physically destroy the drive.

7.3. EDRM

The principles of recovery can be seen from the Electronic Discovery Reference Model (EDRM)[164].



This project was launched in May 2005, to address the lack of standards and guidelines in the electronic discovery market. This problem was identified in the 2003 and 2004 by Socha-Gelbmann in its survey on Electronic Discovery as a major concern for vendors and consumers alike. The completed reference model provides a common, flexible and extensible framework for the development, selection, evaluation and use of electronic discovery products and services.

[164] www.edrm.net\EDRM The statement on its website says "EDRM develops guidelines and standards for e-discovery consumers and providers. From the original model to the current projects, EDRM has helped e-discovery consumers and providers reduce the cost, time and manual work associated with e-discovery".

Expanding on the base defined with the Reference Model, the EDRM projects were expanded in May 2006 to include the EDRM Metrics and the EDRM XML projects. Over the past three years, the EDRM project has comprised more than 118 organizations, including 72 service and software providers, 34 law firms, three industry groups and nine corporations involved with e-discovery.[165] The EDRM working group developed the XML standard which addresses a major problem within e-discovery, namely moving and formatting the different types of data across all of these disparate systems and is "an important step towards streamlining the process".[166]

In total, the new XML standard provides a number of benefits to people involved in all stages of the e-discovery process, including:

- Labour and cost reduction: IT departments, legal teams and service providers no longer have to spend valuable time and resources converting and transferring ESI from system to system.

- Reduction in errors: Not only can organizations focus on proficiency in a single standard schema as opposed to an infinite number of disparate formats, but the validation tool detects non-conforming load files earlier in the process.

- Faster e-discovery process: Data can be transferred from system to system more quickly, ultimately leading to a faster overall process.

- Scalability: The ability to adapt to future technological advances as well as new metadata constructs.

The EDRM project has certainly advanced the process and has gained widespread support.

The process considers various aspects of document retrieval such as:

<u>Location of Electronic Documents</u>
access ability
scope of the search
reasonableness and proportionality
format for production and inspection
any disclosure statement

<u>Non-Compliance with Directions</u>
extent of disclosure: too much or too little
keyword or date or other search parameters
co-operation between the parties
tactics
costs

[165] www.edrm.net\EDRM News » Catalyst Announces Support for EDRM Working Group XML Standard for Electronic Discovery Exchange.mht
[166] George Socha, co-founder of EDRM and president of Socha Consulting LLC http://edrm.net/wiki/index.php/Project_Participants

Other Problem Areas
preservation and/or destruction of documents
identification of documents for preservation and disclosure
identifying the personnel and work practices
governance issues
data protection
privacy concerns

To assist in these issues in the UK, there have been various guidance notes offered and developed in respect of CPR 31 but there are others. It is apparent that all the jurisdictions I have referred to have their own commissions or working parties looking at this subject. However, I would refer you to LiST, the Litigation Support Technology Group[167] data exchange protocol,[168] a copy of which I have provided.

In its release notes the working group states this Protocol is:

> *"a fundamental and important step forward in helping to reduce the costs of electronic data and document exchange within the disclosure process (and, indeed, elsewhere) and we encourage extensive feedback during the consultation period*".[169]

No doubt this Protocol will develop as the process becomes more refined and the software develops to improve the management of the process.

[167] http://www.listgroup.org/ LiST is the Litigation Support Technology Group, an internationally acknowledged UK-based think tank comprising litigation support specialists from numerous law firms and other organisations.

[168] http://www.listgroup.org/documents/Disclosure_Documents_LiST_Group_Data_Exchange_Protocol_1.4_27_April_2007.doc

[169] http://www.listgroup.org/documents/LiST_Protocol_Release_Notes_20070427.doc

8. The Data Handling Process

Let us now turn to various considerations in approaching the data handling process which may affect a tribunal's directions:

8.1. Basic Stages

Retrieval of Data

- the biggest concern is the volume or potential volume
- lack of document management can be a costly hurdle
- facilities to recover outmoded media
- the question of possible corruption of data
- time spent on preparation is the key to effective retrieval

Process of Data

- need to consider how electronic documents can be produced and inspected in a cost effective manner
- consider who should process the data for disclosure
- consider how the searches and tools to be used can reduce the volume of the data
- decide the method of review to be used
- decide how the data will be issued to the other parties
- reviewing the data

8.2. The Main Stages in a Typical Review

Preserve

take backups out of rotation to ensure long-term preservation; consider using image files;

Collect

seek information from clients, custodians and IT team; maintain a chain of custody, avoid opening files to help preserve the integrity of the data;

Index

catalogue files;

Filter and Cull

to filter or cull documents you can select certain types of documents or folders or date ranges or keywords in order to provide a list that meet your requirements;

Process and Remove Duplicates

a function of filtering - Sun systems use the meta data in the file which it records to identify duplicates;

Review Native Files

the use of native files means no costs of conversion to say TIFF format;
some information may be lost on printing as commonly found with excel spreadsheets;
against using native files is that reviewing files in TIFF format can be faster and that redactions can be done immediately;

Redact

you need to convert to TIFF files to allow for redaction which can be lengthy and expensive;

Produce a Timeline

you can use a basic Gantt chart to set out the tasks and monitor progress.

8.3. Costs

It is almost impossible to predict the outcome and the costs of e-disclosure at the outset as various variables need to be estimated. For example, but not limited to:

- the capacity of the typical media;
- the cost of filtering and removing duplication.

Documents and pages per gigabyte are generally considered to be around 20,000 to 30,000 at an average but some files types can be 60,000 pages per gigabyte and if the estimate is wrong, the time and costs can be greatly increased.

8.4. Overall Considerations

To try and improve the process it is necessary to allocate the documents sensibly using well designed software. The team carrying out the review, needs to be properly briefed and monitored. It may help if the review is carried out at different levels rather than one mass intensive review. In this event, priorities for documents could be best and maybe even sampling.

The choice of software is also another consideration. The more human involvement by way of clicking icons or typing in descriptions, results in the review being much slower and hence more costly. Therefore, you need a more automated facility to import information automatically and an easy way of navigating between parent documents and attachments. For example do users need to see the whole of an e-mail thread? Or just the current page? In one case I had recently, the whole contract was controlled by exchange of emails, with some being 14 pages long as people had just tagged response to obtain the recipients name. Hence, as the context was lost, the emails were catalogued in relation to the current sent email. Even so the ‘first page’ of the relevant emails still fully filled 16 lever arch files.

As part of the review process, the question of relevance and even privilege will occur. Once the review has identified documents relevant to issues, those documents themselves can be reviewed a second time and thus may provide a more consistent outcome with senior lawyers concentrating on the key documents that have been produced by this process.

If the process is outsourced, clear instructions will have to be given and in larger cases possibly given in manageable stages. In such case it would be preferable that disclosure is given in agreed stages which will require agreement by the other party in setting out the parameters of the whole process. In selecting an outsource facility I do believe that price should not be the only criteria. Experience in handling the type of case in terms of size, complexity, media, etc should in my view be a more relevant base for selection.

The outsource contract could be negotiated in terms of costs or discounts above or below certain volumes of data. Other considerations may be that in international disputes some of the documents are in more than one language, or that file types are variable as is the format of the document within the file and thus its overall size. Some documents may be protected so they do not have a searchable text. Voice recordings & voicemail tapes etc also need to be considered.[170]

[170] http://www.guidancesoftware.com/ediscovery/discovery.aspx

9. Summary and Recommendations

I hope I have given a background to the e-disclosure/discovery process which seems to be developing its own industry on a worldwide basis with commissions, conferences, working parties and the like being formed around the world. The common factor seems to be an attempt to reduce costs from the process by restricting and managing the disclosure process by the tribunal.

I know we have all encountered situations whereby we have been faced with extensive bundles even after giving directions for just a core bundle, only to find that the documents used in the proceedings could be contained in a single A4 binder. However, we have all heard of tales about solicitors allegedly earning their profits from their copying bill and so I am in favour of making specific orders for disclosure in an electronic form from which the other side can select the documents upon which it wishes to rely. I have tried this on a couple of occasions and it worked quite well except that despite my efforts the parties adopted differing systems of pagination in the core bundles and their closing submissions. I now issue directions that I have one file of paginated documents used during the hearing which both parties must use in their closing submissions.

If you find that directions are required on e-discovery I have in preparing this paper found that there appears to be a growing number of specialist firms that advertise their services. I have therefore, by way of information, listed below the names of some firms and/or practices that say they specialise in this area but as I do not have any personal knowledge of them I am able to provide the links without any fear of favour or in any specific order[171]:
http://www.cy4or.co.uk/ , http://www.fieldsassociates.co.uk/about-us.html , http://www.foxdata.co.uk/index.htm ; http://www.legalinc.co.uk/ ; http://www.millnet.co.uk ; http://www.trilantic.co.uk/contact_us/index.html

As regards adopting a procedure I have already mentioned the Chartered Institute of Arbitrators Protocol, and having considered what else is currently available it does seem to me to be a realistic and understandable procedure and I look forward to using it in the future.

Thank you for your attention.

[171] Information supplied on the understanding that no implied or express warranties or recommendations are given.