Fermin Aldabe v Standard Chartered Bank
[2009] SGHC 194

Case Number : Suit 174/2009, SUM 3788/2009

Decision Date : 27 August 2009

Tribunal/Court : High Court

Coram : Yeong Zee Kin SAR

Counsel Name(s) : Fermin Aldabe, the plaintiff in person; Herman Jeremiah, Choo Hua Yi and Wong Wai Han (Rodyk & Davidson) for the defendant

Parties : Fermin Aldabe — Standard Chartered Bank

Civil Procedure – Disclosure of documents – Providing electronic copies of electronically stored documents

Civil Procedure – Disclosure of documents – Enumeration of e-mails in lists of documents

Civil Procedure – Discovery of documents – Practice of providing copies and deferring physical inspection

Civil Procedure – Discovery of documents – Electronic discovery

Civil Procedure – Discovery of documents – Specific discovery of copies in backup storage

Civil Procedure – Discovery of documents – Specific discovery of earlier e-mails contained in e-mail messages discovery of which has been given

Civil Procedure – Discovery of documents – Discovery of electronically stored documents and databases

Civil Procedure – Inspection of electronically stored documents – Providing reasonable technical means and assistance

Evidence – Documentary evidence – When to raise issues relating to authenticity

Evidence – Computer Output – When to consider issues under section 35 of the Evidence Act

27 August 2009

Yeong Zee Kin SAR:

Introduction

1 The present application was taken out by the Defendant for an order to allow it to give inspection of e-mails listed in its own List of Documents dated 19 June 2009 either by providing printed copies of the e-mails or by providing them in electronic form. Additionally, the Defendant applies for an order that authentication of such copies shall be by certification of the person responsible for the operation or management of the Defendant's e-mail system pursuant to section 35(1)(c) and section 35(6) of the Evidence Act. This application raises interesting issues relating to the difference between discovery of e-mail messages and e-mail mailboxes, inspection of electronically stored documents (including metadata information) and the provision of copies of electronically stored documents within the discovery process.

2 In order to appreciate the rationale for this application, it is necessary for me to set out briefly

the salient procedural history.

Procedural history

3 This is a claim by the Plaintiff against the Defendant for wrongful termination of employment. During pre-trial conference on 15 May 2009, directions were given for discovery to be carried out by exchanging lists of documents by 19 June 2009 and for inspection by 3 July 2009.

4 The Defendant filed its List of Documents ("LOD") on 19 June 2009. On the same day, a copy of the LOD was served on the Plaintiff under cover of a letter wherein the Defendant proposed that parties exchange copies of documents listed in their respective lists of documents by 4 pm on 23 June 2009; if either party required inspection of any original documents thereafter, then arrangements for such inspection was to be made during the week of 29 June 2009. This was followed by an e-mail reminder on 21 June 2009.

5 On 22 June 2009, the Plaintiff replied by e-mail proposing that documents be exchanged at 4:00 pm on 3 July 2009. Later that day, the Defendant's solicitors replied suggesting that parties exchange copies of documents and conduct mutual inspection of the other party's original documents at 4:00 pm on 3 July 2009 at the Central Atrium Basement of the Supreme Court Building. The Plaintiff replied on 23 June, counter-proposing that the meeting be held at 8:30 am and stating that he required physical inspection of all of the Defendant's listed documents.

6 The Defendant's solicitors reply on 29 June 2009 substantively re-iterated their conditions set out in their e-mail of 22 June 2009: the meeting was to be in the afternoon of 3 July 2009 and that parties would exchange copies of documents and provide mutual inspection of original documents. The Plaintiff replied on the same day and raised the issue of inspection of e-mails:

> Regarding inspection emails, do you have access to the email boxes of your client? If not how do you propose to verify the integrity of the email.

7 The Plaintiff proposed delaying inspection until directions could be sought during a pre-trial conference scheduled on 10 July 2009. There were several exchanges of e-mail correspondence between the Plaintiff and Defendant's solicitors between 20 June and 2 July without any resolution of the issue of inspection. On 2 July 2009, the Plaintiff again suggested postponing inspection until after the pre-trial conference scheduled on 10 July 2009 on, *inter alia*, the ground that:

> You are not ready to show documents in their original form and it is futile to do inspection twice.

8 On the same day, the Defendant agreed to postponement of inspection. During pre-trial conference on 10 July 2009, the Defendant was directed to file an application for leave to dispense with the usual mode of inspection.

9 At the hearing of this application before me on 11 August 2009, the Defendant's solicitors proceeded on the basis that the Plaintiff had made a request for the inspection of the Defendant's employees' e-mail mailboxes and sought an order that inspection of e-mail messages be provided by either printed copies of the e-mails or electronic copies of the e-mails. The Defendant solicitors also raised a preliminary issue as to whether the Plaintiff had waived his right to physical inspection of the e-mail messages listed in the Defendant's LOD by reason of an admission provided by the Defendant.

10 On the preliminary issue, I gave *ex tempore* grounds for holding that the Plaintiff did not waive his right to inspection, which I reproduce herewith in full:

> Based on the sequence of correspondence placed before me, I do not think that there was any agreement between parties on the proposal for an admission in exchange for waiver of inspection. I would characterise the e-mail proposal of the Plaintiff dated 11 July 2009 as an offer which was rejected by conduct when this application was filed on 17 July 2009. I am particularly persuaded by the fact that there were no attempts to negotiate between parties during the period between 11 and 17 July, even though the Plaintiff was in Singapore. As such I do not think that the letter from Defendant's solicitors dated 30 July 2009 amounted to an acceptance of the offer. The correspondence will remain; although I had observed that the significance of who provided pen and paper escapes me at this point.

11 I do not intend to revisit this preliminary issue in these grounds of decision, which is intended to deal with the substantive issues raised in the application.

Outline of issues

12 The issues before me may be summarised as follows. First, what was the subject matter of the inspection order which is sought? Is the Defendant required to give inspection of the entire mailboxes of the employees of the Defendant, whose e-mails had been listed in the Defendant's LOD filed on 19 June 2009, or was inspection only to be ordered in respect of the individual e-mail messages which were enumerated? Second, how should inspection of e-mail messages be given? This raised subsidiary issues relating to the common practice of giving inspection by providing copies of the discoverable documents first and deferring physical inspection. How should this practice be adapted for documents which are stored electronically?

Inspection of individual e-mails or entire mailboxes

13 The first issue is whether inspection should be ordered in respect of the 153 e-mail messages listed in the Defendant's LOD or the entire mailboxes of the 14 employees concerned with these e-mail messages. It is beyond doubt that individual e-mail messages are treated as separate documents and may be discoverable as such. For example, e-mail messages were part of the correspondence discovered in *PSA Corp Ltd v Korea Exchange Bank* [2002] 3 SLR 37; [2002] SGHC 88. In *Trek Technology (Singapore) Pte Ltd v FE Global Electronics Pte Ltd and Others and Another Suit* [2003] 3 SLR 685; [2003] SGHC 185, internal e-mail messages were treated as discoverable, although it was held that discovery of internal e-mails was unnecessary at the stage of the proceedings when the application was brought but the judge left it open for a further application for discovery of internal e-mails to be made before the trial judge. In *K Solutions Pte Ltd v National University of Singapore* [2009] SGHC 143, it was observed (at paragraph 14) that "email … [was] treated as documents and it was accepted that the discovery obligations of the parties extended to disclosure of relevant email …".

14 It is equally beyond doubt that databases are discoverable and hence liable to production for inspection. In *Alliance Management SA v Pendleton Lane P and Another and Another Suit* [2007] 4 SLR 343; [2007] SGHC 133, it was observed (at paragraph 10) that:

It is convenient at the outset to restate the principles that would apply when approaching the issues here. First, it bears noting that Vinelott J in *Derby & Co Ltd v Weldon (No 9)* [1991] 1 WLR 652 ("Derby No 9") concluded that material on a computer database constituted a "document" within O 24. The word "document" covers "anything upon which evidence or information is recorded in a manner intelligible to the senses or capable of being made intelligible by the use of equipment" (see Singapore Civil Procedure 2003 (G P Selvam ed) (Sweet & Maxwell, 2003) at para 24/1/2). A "document" is defined in s 3(1) of the Evidence Act (Cap 97, 1997 Rev Ed) as "any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of those means intended to be used or which may be used for the purpose of recording that matter". Material stored on a computer database is within this definition. Yong Pung How CJ in *Megastar Entertainment Pte Ltd v Odex Pte Ltd* [2005] 3 SLR 91 at [34] reviewed the definition of "document" in the Evidence Act and other statutes and, inter alia, concluded that as with the other statutes considered in that case, the Evidence Act definition of the word "document" was broad enough to encompass information recorded in an electronic medium or recording device such as a hard disk drive installed in a desktop or server computer. Put simply, the concept of "document" embraces the Hard Disk for the purposes of O 24 of the ROC.

15 Individual e-mail messages are sent and received using e-mail accounts which are maintained on e-mail servers. E-mail systems generally fall within two broad categories: those based on Internet standards and proprietary e-mail systems. Internet e-mail systems make use of the Multipurpose Internet Mail Extensions (MIME) standards for the e-mail message format, the Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and/or Internet Message Access Protocol (IMAP) to send and receive e-mails. Proprietary e-mail systems, as the name suggests, make use of proprietary protocols; examples of proprietary e-mail systems are Lotus Notes and Microsoft Exchange. E-mail accounts are accessed using client software programs. Web-based e-mail systems (or Webmail) on the other hand are designed to be accessible using web browsers. (See generally, "E-mail" from Wikipedia, the free encyclopedia, at: <http://en.wikipedia.org/wiki/E-mail>.)

16 Depending on how the e-mail client software program is configured, a copy of the e-mails sent or received in an e-mail account may be stored on the hard disk of the personal computer of the user or in the e-mail account on the e-mail server, or both. An e-mail mailbox is a metaphor which is employed by e-mail client software to represent e-mail messages in the e-mail account. The typical e-mail mailbox may include an Inbox, Outbox, Sent and Draft folders (ie default folders); e-mail client software typically permit the user to organise e-mails into folders (ie user-defined folders).

17 A database is no more than "a collection of data arranged for ease and speed of search and retrieval": definition of "database" in TheFreeDictionary, at <http://www.tfd.com/database>. As each mailbox contains a collection of individual e-mail messages arranged in either the default or user-defined folders, each mailbox may be treated as a database of individual e-mail messages.

18 Put another way, the first issue is the difference between inspection of 153 e-mail messages as individual documents or 14 mailboxes as databases.

19 While the application was ostensibly one for inspection of individual e-mails, submissions had initially proceeded on the basis of inspection of the entire mailboxes of certain of the Defendant's employees whose e-mails were listed in the Defendant's LOD filed on 19 June 2009. This was the result of the Defendant's interpretation of the Plaintiff's request in his e-mail dated 29 June 2009 (which has been reproduced above) as a request for discovery of the entire mailbox of each employee

who had either sent or received the e-mails which were listed in the Defendant's LOD. Solicitors for the Defendant objected to inspection of the entire mailboxes of these employees principally on two grounds.

20 First, the number of relevant e-mails (in the context of the entire mailbox of each employee) was small. During submissions, Defendant's solicitors highlighted that of the 153 e-mails disclosed by the Defendant in its LOD, these resided in the mailboxes of 14 of the Defendant's employees; 9 of these employees are based in Singapore and 5 are based in London. The vast majority of the e-mails contained in the mailboxes of these employees are irrelevant to the present action.

21 Second, there were other e-mails in the mailboxes of these employees which were subject to banking secrecy and/or confidentiality obligations. Most of these employees who are based in Singapore were from the Human Resource Department and their e-mails dealt with confidential information relating to other employees of the Defendant. Most of these employees who are based in London are from the Market Risk Function and deal with highly confidential information relating to the Defendant's operations, some of which information are protected under banking secrecy laws.

22 As observed in *Alliance Management SA v Pendleton Lane P and Another and Another Suit* [2007] 4 SLR 343; [2007] SGHC 133 (at paragraph 18), there is a distinction between the court's power to order discovery of information in a database and its discretion to order production of the database for the purposes of inspection. In that case, the database concerned was a hard disk drive. As inspection of an entire database is far more intrusive than discovery and inspection of specified information contained therein, the judicial inquiry:

> is a far more intricate one involving judicial balancing of the competing interests of the parties; ie, the requesting party's right to reasonable access to documents that are necessary to conduct his case without unduly burdening the other party in terms of time and expense and to prevent unauthorised "trawling" through the database. (at paragraph 19)

23 A request for discovery and inspection of a database has to be clearly made. If the database was the subject of a discovery order or if it was listed as such in a list of document, there can be no doubt. Alternatively, it is possible that although not specifically ordered or listed, there is no doubt between the parties that discovery and inspection of the database is sought. In *Alliance Management SA v Pendleton Lane P and Another and Another Suit*, the history of the discovery battles between parties made it clear that inspection of the hard disk was sought. Hence, despite the fact that the list of documents contained a compendious list of 36,740 documents retrieved from key word searches and the application was for discovery and inspection of these documents, it was clear to the parties that the heart of the application was for inspection of the hard disk.

24 Based on my perusal of the correspondence between parties, I do not understand the Plaintiff to have requested for inspection of entire mailboxes. Taken together, the Plaintiff's e-mails dated 29 June and 2 July 2009 amounted to a request for the direct inspection of individual e-mail messages listed in the Defendant's LOD from the mailboxes of the relevant employees of the Defendant. Granted that the Plaintiff had not identified which of the 153 e-mail messages he wanted to inspect, I do not think that this lack of specificity converted his request to one for inspection of the entire mailboxes of all 14 employees. On the contrary, I think that the natural inference is that the Plaintiff intended to request for inspection of all 153 e-mail messages.

25 Indeed, in the course of submissions, the Plaintiff clarified that he wished only to inspect 14 e-mails in order to view the e-mail header, in particular the routing information. The e-mail header

contains, *inter alia*, metadata information relating to who sent the e-mail, who it was addressed to, who were copied on the e-mail and information which track the various e-mail servers which have previously handled that particular e-mail (ie routing information). Accordingly, I directed that the Plaintiff identify these e-mails and he duly identified them to be the e-mails listed at serial numbers 71, 73, 88, 90–96, 100, 105, 106 and 108 of the Defendant's LOD.

Inspection of electronically stored documents

26 The second issue is to determine how inspection of individual e-mail messages is to be given. This raises subsidiary issues relating to how the common practice of giving inspection by providing copies of the discoverable documents first, and deferring physical inspection of specified documents may be adapted for electronically stored documents.

Discovery and inspection: law and practice

27 Without delving into the case law relating to discovery, I propose first to set out briefly the classical sequence in which discovery and inspection takes place under Order 24. Discovery of documents is given by enumerating them in a list of documents, the completeness of which is to be verified by affidavit. The list typically contains a notice stating the time and place at which the party served with the notice may inspect the documents referred to in the list. The list and affidavit verifying are served on the other parties in the action. At the appointed time and place, the enumerated documents are produced for physical inspection and the inspecting party is entitled to take a copy of the inspected documents during inspection.

28 Hence, inspection and the taking of copies occurs concurrently in the classical sequence. However, there is a common practice for parties to agree that copies of all documents enumerated in each party's list of documents be exchanged first and for physical inspection of documents to be deferred. After copies of documents have been exchanged, a party is still entitled to request for inspection of specified documents pursuant to the agreement to defer physical inspection. Vide their letter of 19 June 2009, the Defendant's solicitors had initially proposed that inspection be carried out in precisely this fashion: see paragraph 4.

29 The Defendant's application departs from both the classical sequence as well as the common practice for inspection as it prays for inspection to be given "by providing to the Plaintiff inspection of paper printouts" or alternatively "by providing to the Plaintiff inspection of CD-ROMs containing electronic copies" of the enumerated e-mail messages. I understood this to mean that once copies were provided, there would be no physical inspection. During submissions, Defendant's solicitors were quite prepared to take a practical approach in accordance with the common practice for the giving of copies first followed by inspection.

30 To my mind, it makes no difference whether inspection is given in the classical sequence or in accordance with the common practice. Inspection should be approached in a practical manner. Where discovery reveals that only a minority of documents in the possession of the disclosing party is required by the inspecting party, it may be more practical to adopt the classical sequence whereby such documents are produced for the inspecting party to determine whether a copy needs to be taken. On the other hand, where the volume of documents is high or where copies of the majority of documents given in discovery is required, it may make more sense for inspection to be deferred and for copies to be exchanged in accordance with the common practice. So far as electronically stored documents are concerned, the unique issues arise not in the sequence of inspection and the taking of copies, but in how inspection should be carried out and copies given.

Providing copies of electronically stored documents

31 Where documents are stored in an electronic form, it is preferable that copies be provided in an electronic form. Given the vast amount of electronically stored documents that are discovered these days during the course of litigation, the practice of giving copies of these documents in print or as printouts should be discouraged. Practice Direction 3 of 2009 (which, though issued on 30 July 2009 does not take effect until 1 October 2009 and is thus not applicable to this application) prefers the supply of copies of electronic copies of discoverable documents in their native format: paragraph 43G. Parties may agree on another electronic format for the supply of copies. The rationale is simple: particularly where discoverable documents are voluminous, it does not make sense to generate reams of printout of electronic documents. The provision of copies of electronic documents in their native format also has its benefits, *inter alia*, ease of transfer (it is easier to transfer electronic documents in optical discs as opposed to cartons of printouts), the preservation of metadata information that is part of the native format and enabling the inspecting party to conduct keyword searches (if the native format is text-searchable).

32 In the present case, the Defendant had prayed alternatively for the provision of copies of the discoverable e-mail messages either in printouts or in electronic form in the Personal Storage Table ("PST") format. The Plaintiff intimated during submissions that he had all of his documents in the Portable Document Format ("PDF") and he was prepared to exchange documents electronically. Although the number of e-mail messages in the present case was not many, I was (for reasons set out above) of the view that electronic exchange of discoverable documents should be ordered.

The practical necessity for parties to discuss electronic discovery issues

33 There was however still the issue of the exchange format for these e-mail messages. The Defendant uses Microsoft Outlook as their e-mail client software and proposed to deposit the discoverable e-mail messages from the mailboxes of the employees concerned into specially created PST files. The Plaintiff is unable to accept this as he uses a Linux computer and is unable to read PST files. He requested that copies be exchanged in PDF format instead. It was evident that solicitors for the Defendant were not able to make a decision as to whether it was feasible to provide copies of the discoverable e-mail messages as PDF files without consulting with the IT department of their client. This highlights an important practical hurdle that is thrown up in electronic discovery which is not so apparent in the discovery of documents which exists in paper form.

34 Although the provision of electronic copies of discoverable electronically stored documents in their native format forms the default position in Practice Direction 3 of 2009, parties are able to agree on another exchange format: paragraph 43G. The rationale is that occasionally, the native format is not accessible to the party entitled to copies. This may be because the native format is obsolete and the software required to access it is not readily available or the native format may be proprietary, requiring the inspecting party to acquire proprietary software in order to access the documents. In the present case, the Plaintiff submitted that the PST format is proprietary and required Microsoft products, namely Outlook, in order to access it. As the Plaintiff was an individual and was conducting these proceedings personally, he does not have the same financial muscle as the Defendant. It is desirable that the e-mails messages be provided to him in a manner which he is able to access with reasonable ease. However, by converting the e-mail messages into PDF files, there is a risk that metadata information, namely header information, may be lost in that process. The Plaintiff submitted that it is possible to convert the e-mail messages in a manner such that the metadata information would be visible in the resulting PDF document. Again, it was evident that solicitors for the Defendant were not able to commit until they have had an opportunity to consult with the IT department of their client.

35 It was clear to my mind that it was necessary for parties to meet for the purpose of discussing these technical issues. In Practice Direction 3 of 2009, parties are "encouraged to collaborate in good faith and agree on issues relating to the discovery and inspection of electronically stored documents"; and to do so immediately after the close of pleadings and before the automatic directions for discovery in Order 25, rule 8 takes effect: paragraph 43B. This is an approach which mirrors the approach taken in both the United States and United Kingdom. Under paragraph 2A.2 of the Practice Direction to Part 31 of the UK Civil Procedural Rules, parties are required to discuss any issues that may arise regarding searches for and the preservation of electronic documents before the first Case Management Conference. Additionally, parties are also to co-operate at an early stage as to the format in which electronic copy documents are to be provided: paragraph 2A.3. A similar process is set out in Rule 26(f) of the US Federal Rules of Civil Procedure. An obligation is placed on parties to confer, 21 days before a scheduling conference, to discuss any issues relating to preserving discoverable information and to develop a discovery plan that addresses, *inter alia*, "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced". Indeed, in the recent decision in *Digicel (St. Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), at [47], the court highlighted the potential pitfalls where parties fail to meet for discussion:

> This case provides an opportunity for the Court to emphasise something mentioned in Part 31 Practice Direction which the parties in the present case disregarded. Paragraph 2A.2 of the Practice Direction states that the parties should at an early stage in the litigation discuss issues that may arise regarding searches for electronic documents. Paragraph 2A.5 of the PD states that where key word searches are used they should be agreed as far as possible between the parties. Neither side paid attention to this advice. In this application the focus is upon the steps taken by the Defendants. They did not discuss the issues that might arise regarding searches for electronic documents and they used key word searches which they had not agreed in advance or attempted to agree in advance with the Claimants. *The result is that the unilateral decisions made by the Defendants' solicitors are now under challenge* and need to be scrutinised by the Court. If the Court takes the view that the Defendants' solicitors' key word searches were inadequate when they were first carried out and that a wider search should have been carried out, the Defendants' solicitors' unilateral action has exposed the Defendants to the risk that the Court may require the exercise of searching to be done a second time, *with the overall cost of two searches being significantly higher than the cost of a wider search carried out on the first occasion*. (Emphasis mine.)

36 Although this exhortation was made in the context of key word searches, I think that the warning applies with equal force to issue of the format in which copies of electronic documents are to be provided. *Bona fides* discussions between parties may avoid wastage of time and resources, and avert legal costs. I therefore made certain directions (which are reproduced below) for parties to meet and discuss the format for the exchange of electronic copies of documents enumerated in their respective lists of document, and how such exchange may be carried out. As the Plaintiff was prepared to accept e-mail messages in PDF format, that was to be the preferred format for exchange of electronic copies of e-mail messages, subject to parties' agreement.

Inspection of electronically stored documents

37 On the issue of the manner of giving inspection of e-mail messages, the Defendant was concerned that allowing the Plaintiff access to the e-mail mailboxes of its employees will breach confidentiality and banking secrecy. The Defendant relied on Vinelott J's observations in *Derby & Co*

Ltd v Weldon (No 9) [1991] 1 WLR 652 (at pages 658E–659D), to highlight some difficulties in providing inspection in this manner. Briefly the difficulties highlighted are: first, that the inspecting party may gain access to privileged material; and second, whether access can be arranged and if so, whether the granting of access may unduly interrupt the necessary daily use of the computer. On this basis, Defendant's solicitors sought to argue that inspection was not necessary. To avoid such difficulties, the Defendant proposed that inspection be given by providing electronic copies of the discoverable e-mail messages in PST format, in lieu of physical inspection.

38 This was not acceptable to the Plaintiff as he was not able to access PST files. Additionally, he wanted to be able to view the e-mail header information which will show the routing history of the e-mail messages. His concerns related to issues of authenticity which I will deal with later.

39 To my mind, I did not agree that a party's obligation to give inspection can be fulfilled by the provision of copies. In the course of submissions, I had made it clear to parties that we were only concerned with inspection of e-mail messages enumerated in a list of documents, not e-mail mailboxes. I had also indicated that the provision of copies and inspection should take place as originally proposed by the Defendants in their letter of 19 June 2009: viz, in accordance with the common practice of providing copies first and deferring physical inspection to a later time. The Plaintiff cannot be disentitled to physical inspection even if he had been provided with copies. Further, since he had identified 14 e-mail messages, I did not think that giving inspection of these e-mail messages would present any major difficulties or incur unnecessary costs.

40 Moving on to the question of how inspection should be provided, I drew an analogy with the traditional manner of giving inspection for hardcopy documents. At the appointed time and place for inspection, the hardcopy documents would be provided to the inspecting party who is then at liberty to physically inspect the documents (and to take copies if copies had not already been provided). It has been held (in the context of inspection of documentary samples by experts) that inspection is not limited to ocular examination and equipment may be used to inspect documents: *per* Sundaresh Menon JC, in *UMCI Ltd v Tokio Marine & Fire Insurance Co (Singapore) Pte Ltd and Others* [2006] 4 SLR 95; [2006] SGHC 142, at [66]. In *Grant and Another v Southwestern and County Properties Ltd and Another* [1975] 1 Ch 185, the court had to decide whether a tape recording was a document which was discoverable. In holding that a tape recording was a document for the purposes of discovery, Walton J observed as follows (at page 198C-F):

> … it seems to me that the simplest and most foolproof method of "inspection" in these cases is for the party giving discovery to play the tape to the party to whom discovery is being given, and for that party to make his own recording as it is played.

41 The principle of law which was articulated here is that where a document cannot be meaningfully examined by ocular examination, the party giving discovery has an obligation to provide the technical means necessary in order to give effect to the inspecting party's right of inspection. This is the approach which is adopted in Practice Direction 3 of 2009: the party producing electronically stored documents has to provide reasonable means and assistance for inspection (paragraph 43F).

42 In the present case, the e-mail messages are stored electronically on the Defendant's e-mail servers. The Defendant has to provide the technical means necessary in order to give effect to the Plaintiff's right to inspect the 14 e-mail messages which he had identified. At a minimum, the Defendant has to provide a computer system from which the relevant e-mail mailboxes may be accessed and the 14 e-mail messages displayed on screen for the Plaintiff to view. However, this is not to say that the Plaintiff would be given full access to the e-mail mailboxes of the Defendant's

employees. I am mindful of Vinelott J's observations in *Derby & Co Ltd v Weldon (No 9)* [1991] 1 WLR 652 concerning the difficulties in providing inspection of databases, and also of the Defendant's concerns of breaches of confidentiality and banking secrecy. The Plaintiff had also articulated his intention to view the header information of the 14 e-mail messages. I thought that a sensible approach would be for the Defendant to assist by providing an operator who would retrieve each of these 14 e-mail messages and display them on screen for the Plaintiff's inspection, and call up the metadata information (eg header information) which the Plaintiff intended to inspect. However, it is prudent for the Defendant to be given an opportunity to review the metadata information for the purpose of determining if there was any basis for objecting to production for inspection before it is shown to the Plaintiff.

43 Having in mind the practical issues which needed to be addressed, I directed that parties meet for the purpose of discussing and agreeing on a protocol for the provision of copies of documents enumerated in the lists of documents and for the physical inspection of e-mail messages. In order to assist parties in reaching agreement, I further directed that the protocols were to be drawn up within the following framework which is now reproduced in full:

> First, parties are to exchange copies of documents that have been listed in their lists of documents in an electronic format to be agreed. Within the next 7 days, parties are to meet for the purpose of discussing the following issues:
>
> (a) identifying the documents in the counterparty's list of documents for which copies are required;
>
> (b) the electronic file format for providing copies – for documents which are in hardcopy, the preference would be for photocopies; for documents which are not e-mails, the preference would be for the native format of the documents; for e-mails, the preference would be for exchange in PDF format; and
>
> (c) the manner of exchange of electronic copies – the preference will be for exchange in CD-ROM.
>
> Second, inspection will be provided by the Defendant of the following documents listed in the Defendant's List of Documents filed on 19 June 2009: s/no 71, 73, 88, 91, 92, 93, 94, 95, 96, 100, 105, 106, 108 and 90.
>
> Parties are to agree on a protocol for inspection within the following framework:
>
> (a) the Defendant will provide reasonable access to the e-mails which are to be produced for inspection;
>
> (b) inspection will be carried out in the presence of solicitors for the Defendant and representatives of the Defendant, together with the Plaintiff;
>
> (c) the Defendant will provide an operator who will retrieve and call up the e-mails which have been identified for inspection and to present the e-mails on screen;

(d) the Plaintiff may request for the display of hidden or non-visible metadata information like header information – the Defendant will be entitled to seek advice on privilege, banking secrecy or any other basis for objection before giving instructions to the Defendant's operator to present the metadata information on screen for the Plaintiff to inspect.

44 I adjourned the matter for a week for parties to agree on the text of the protocols.

Adjourned hearing on 19 August 2009

45 At the adjourned hearing on 19 August 2009, parties updated the court that they had agreed that all documents would be exchanged in text-searchable PDF format. The Defendant raised two technical issues.

Scope of inspection

46 The first issue was that not all the e-mail messages that are referred to in their LOD are stored on e-mail servers. It was explained that each employee has to keep his e-mail mailbox on the e-mail servers within a certain size. When that size is reached, e-mails are transferred from the e-mail servers into PST files which are stored on the hard disk of the employee's personal computer or notebook. In order to provide inspection, arrangements had to be made for the e-mail servers, personal computers or notebooks to be available. The difficulty lies in that some of these are in London and different levels of internal approvals and (for personal computers and notebooks) the consent of the employees concerned had to be obtained before they can be made available for inspection. There would also be additional costs involved in arranging for the e-mail servers, personal computers and notebooks situated in London to be available for inspection via remote access from Singapore. For the purposes of discovery, the Defendant's Singapore office had been provided with hard copy printouts as well as a PST file containing electronic copies of these e-mail messages by its London offices.

47 The Plaintiff raised issue with inspecting PST files which touch on authenticity. This will be dealt with below.

48 I approached this issue in the following manner. The Defendant had described these e-mail messages as copies in its LOD. To my mind, it was plain that the copies which the Defendant had given discovery of were either the hard copy printouts or the electronic copies residing in the PST file which they had in their possession in Singapore. Inspection should therefore be of the either the hardcopy printouts or the electronic copies in the PST file. As the documents which were referred to in the Defendant's LOD were the copies in their possession in Singapore, I did not see any reason at this stage to order inspection of the e-mails residing in e-mail servers, personal computers or notebooks in London. Since the Plaintiff's reason for inspection is to view metadata information, I ordered that inspection of e-mail messages of employees based in London be given from the PST file in the possession of the Defendants.

Challenges to authentication

49 In the course of submissions, the Plaintiff raised what amounted to attempts to challenge the authenticity of e-mail messages which had been transferred from e-mail server to PST files. In brief, the basis for his attempts to challenge authenticity was that once e-mail messages have been transferred to the hard disk of an employee's personal computer or notebook, it is possible for the

employee to alter the contents of the e-mail messages. He further requested that copies of these e-mail messages which are stored in the Defendant's backup storage be produced to prove authenticity.

50 His attempt to challenge authenticity may be dealt with succinctly. The proper juncture for him to put authenticity in issue is *after* inspection (or the time limited for inspection) by serving a notice under Order 27, rule 4. This provides notice to the Defendant that it has to call the appropriate witnesses to prove authenticity of the disputed documents (including e-mail messages) *at the trial*.

51 Similarly, his attempt to request for specific discovery of copies of the e-mails in the Defendant's backup storage may also be dealt with shortly. Unless he is able to provide some basis for believing that the Defendant has backup storage and copies of these e-mails exists therein, his request for specific discovery cannot get off the ground. This should rightfully be the subject of a separate specific discovery application after inspection is complete. The onus is on the Plaintiff to show that retrieval of copies of the identified e-mail messages from the Defendant's backup storage is necessary either for the fair disposal of the action or for saving costs.

52 This brings me to the Defendant's application, which prays for an order that copies of e-mail messages given in discovery be duly authenticated by certification of a person responsible for the operation or management of the Defendant's relevant computer system. This too is premature. Compliance with section 35 of the Evidence Act is an evidential matter that should rightfully be addressed at trial.

53 In the present case, the proper manner for the Plaintiff to approach the issue of authenticity is to identify, *during the course of inspection*, the documents which he intends to challenge; he puts authenticity in issue by serving on the Defendant a notice under Order 27, rule 4. The Defendant would then have to prove the e-mail messages, the authenticity of which have been challenged, in the usual way – by calling the appropriate witnesses for the trial: *Jet Holding Ltd and Others v Cooper Cameron (Singapore) Pte Ltd and Another and Other Appeals* [2006] 3 SLR 769; [2006] SGCA 20. Whether copies of the challenged e-mail messages should be recovered from the Defendant's backup storage is an evidential matter for the Defendant to decide for the purpose of proving authenticity.

54 In *Lim Mong Hong v Public Prosecutor* [2003] 3 SLR 88; [2003] SGHC 161, it was held that section 35 of the Evidence Act applies to all forms of computer output evidence, both real evidence and hearsay evidence. The Defendant has an affirmative duty to adduce evidence that the relevant computer systems were working properly. As parties head towards trial, evidential issues will have to be addressed. Section 35(1)(a) provides a situation where parties, in the lead up to or even during the trial, come to an agreement not to dispute authenticity or accuracy of some or all of the e-mail messages. This may take the form of, for example, an agreed bundle of documents where both authenticity and accuracy are not disputed. Alternatively, the Defendant may produce a certificate signed by a person holding a responsible position in relation to the operation or management of the relevant e-mail server, personal computer or notebook in order to admit the e-mail messages. Finally, if the copies of the e-mail messages were reproduced in an approved process, the Defendant may produce a certificate signed by a person holding a responsible position in relation to the operation or management of the approved process. To my mind, as issues are crystallised in the course of proceedings and as parties prepare for trial, it is very possible that parties may agree to authenticity of a majority of electronically stored documents (including e-mail messages); there may even be agreement as to the content (ie accuracy) of some of the electronically stored documents. Some of the documents referred to in the Defendant's LOD may form part of an agreed bundle of documents, which may be admissible by agreement under section 35(1)(a) of the Evidence Act. For these reasons, I do not think that it is appropriate for me to make any order relating to the manner in which

the Defendant may comply with section 35 of the Evidence Act at this early stage. Accordingly, I made no orders as to the mode by which copies of electronically stored documents given in discovery should be proved during the trial.

55 As parties had not settled the text of the protocol for the provision of copies of documents enumerated in the lists of documents and for the physical inspection of e-mail messages, I adjourned this matter overnight for them to do so.

Adjourned hearing on 20 August 2009

56 At the adjourned hearing on 20 August 2009, parties had substantially agreed on the text of the protocol for the provision of copies of documents enumerated in the lists of documents and for the physical inspection of e-mail messages, save for timelines. During submissions, a fundamental issue was surfaced.

Manner of describing e-mail messages in lists of documents

57 There was some confusion as to whether inspection was to be given for 14 e-mail messages, or 14 items listed in the Defendant's LOD wherein each item may consist of one or more e-mail messages. Taking item 90 of the Defendant's LOD as an example, it was described in the following manner in the Defendant's LOD:

06.11.08 – 12.11.09	Email exchange between the Plaintiff and Gavin Taylor Email exchange between Gavin Taylor and Simon Gurney Email from Gavin Taylor to Jenny Huang

58 The Plaintiff had understood this to mean that it was an e-mail from Gavin Taylor to him enclosing e-mail messages from Gavin Taylor, Simon Gurney and Jenny Huang. According to the Plaintiff, he had never received any e-mail message which included an e-mail in which Simon Gurney appeared on the address list. He had requested for inspection on this understanding.

59 At the hearing on 19 August 2009, it was explained that item 90 consisted of at least 3 e-mail messages: 2 sets of e-mail exchanges and an e-mail message. As the Plaintiff had identified item 90 for inspection, I was prepared to order that the Defendant give inspection of the 3 (or more) e-mail messages which it had intended item 90 to refer to.

60 A printout of item 90 was tendered at the hearing on 20 August 2009. It turned out that item 90 was a single e-mail message from Gavin Taylor to Jenny Huang, containing 6 earlier e-mail messages. It was unfortunate that the description of the e-mail message referred to as item 90 was not described with sufficient accuracy. To my mind, each item in a list of documents should refer only to a single e-mail message. The e-mail message may be a single message between sender and recipient. However, it is often the case that prior e-mail messages are included in subsequent replies, thereby forming a chain of e-mails. In such situations, if the Defendant is giving discovery only of the most recent e-mail message in the chain, it should be described in a manner that makes it clear that it is a single e-mail message but which contains the contents of several prior e-mail messages. Using item 90 as an example, I think that one possible way to describe it could be as follows:

12 November 2008	E-mail from Gavin Taylor to Jenny Huang enclosing 6 e-mails between 10 November 2008 and 6 November 2008 between Simon Gurney, Gavin Taylor and the Plaintiff

61 Alternatively, if more details are to be inserted, then another possible way to describe it could be as follows:

12 November 2008	E-mail from Gavin Taylor to Jenny Huang enclosing – E-mail from Simon Gurney to Gavin Taylor dated 10 November 2008 4:23 pm E-mail from Gavin Taylor to Simon Gurney dated 10 November 2008 03:29 E-mail from Simon Gurney to Gavin Taylor dated 7 November 2008 9:14 pm E-mail from Gavin Taylor to Simon Gurney dated 7 November 2008 07:17 E-mail from the Plaintiff to Gavin Taylor dated 7 November 2008 4:14 am E-mail from Gavin Taylor to the Plaintiff dated 6 November 2008 7:13 am.

62 The intention of these examples is not to prescribe any particular manner of describing e-mail messages which contains a chain of earlier e-mail messages. They are illustrative of the point that the description should be clear and accurate in order to avoid confusion.

Deferring inspection

63 At this point, the Plaintiff stated that he had requested for inspection of the 14 e-mail messages under a mistaken basis arising from the confusion over how the e-mail messages were described in the Defendant's LOD. He was also under the mistaken view that if an e-mail message contained within it the contents of several prior e-mail messages, he would be able to inspect the metadata information of these e-mail messages separately. I did not think that this was the correct approach.

64 Returning to first principles, where a document contains annexures is given in discovery, inspection will be given for that document including the annexures. If the inspecting party wishes to inspect the original documents which formed part of the annexures, he must make a request for specific discovery. An order for disclosure and inspection will only be made if it is shown that the original of such documents are in the possession, custody or power of the party giving discovery. Applying the same approach to e-mail messages, if the Plaintiff intends to request for inspection of an e-mail message the contents of which is contained in one of the e-mail messages given by the Defendant in discovery, he has to make a specific request. An order for discovery and inspection can only be made if the Defendant has a copy of the requested e-mail message in its possession, custody or power. He may not have it for various reasons, for example, the employee may have deleted it from his e-mail mailbox without saving a copy in a PST file on his personal computer or notebook. Even if a copy is in the possession, custody or power of the Defendant, it may not be necessary to order

discovery and inspection as it may not be relevant or the cost of recovery of a copy of the requested e-mail message may be disproportionate to the significance of the e-mail message to the issues in dispute.

65 In the end, good sense prevailed and parties agreed to adopt the common practice of giving inspection whereby copies of documents referred to in their respective lists of documents would be exchanged first and deferring inspection by agreement. I need only mention that this case turned out to be an object lesson in the pitfalls in electronic discovery which could have been avoided had parties heeded the admonition in *Digicel (St. Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch) (see above, paragraph 35).

66 Accordingly, I gave directions for the exchange of electronic copies of documents, followed by each party notifying the other of the documents for which inspection should be given and ending with inspection proper. Minor amendments were also directed to the draft protocol for the provision of copies of documents enumerated in the lists of documents and for the physical inspection of e-mail messages and I directed that the protocol form part of the discovery order.