Electronic Disclosure

Mark Humphries, Neil Mirchandani and Sanjay Bhandari[1]

1 The Problem of Disclosure of Electronic Documents

1.1 This paper has been produced for consideration by members of the Commercial Litigators' Forum[2] to address the perceived difficulties of dealing with disclosure of electronic documents in commercial disputes. In particular, the following issues arise.

1.1.1 What is an electronic document?

1.1.2 How do the current Civil Procedure Rules ("**CPR**") on disclosure apply to electronic documents?

1.1.3 What unique problems arise with providing disclosure of electronic documents compared with conventional paper documents?

1.1.4 Do the CPR assist practitioners in addressing the problems associated with disclosure of electronic documents?

1.1.5 How can the court be assisted to understand the scale of the difficulties posed by disclosure of electronic documents in any given case?

1.2 In the remainder of this paper, we seek to address these and other related issues. In summary, and for the reasons that follow, we consider that:

1.2.1 The current definition of 'documents' as it applies to electronic media could be more helpfully clarified;

1.2.2 There is an increasing proliferation of data being stored on electronic media with the increasing use of email and business trends towards paperless (or, at least, less paper intensive) offices;

---

[1] Mark Humphries is head of advocacy at Linklaters in London. Neil Mirchandani is a litigation partner at Lovells in London. Sanjay Bhandari is a senior Associate in the Dispute Resolution Department at Baker & McKenzie in London.

[2] The Commercial Litigators' Forum ("CLF") was established in July 2002 by a number of the leading dispute resolution law firms to promote informal discussion of, and to promulgate initiatives in, dispute resolution related issues affecting the legal profession and the court system. The authors would welcome comments on this paper. Comments can be sent to robin.preston-jones@sjberwin.com. These will be posted on the CLF website www.commerciallitigatorsforum.com.

1.2.3 In any given case, there may be an incredible mass of data held on electronic documents which theoretically fall to be disclosed;

1.2.4 The CPR do not provide much assistance in terms of limiting the scope of the disclosure and inspection exercise in relation to electronic documents: the parties and the court are largely left to deal with this in an *ad hoc* fashion on a case by case basis;

1.2.5 There may be much to be learned from our colleagues in the United States who have grappled with the issue of electronic disclosure for some years and we see some sense in their general approach of considering both accessibility of the documents and whether the costs burden should be shifted to the inspecting party in appropriate circumstances;

1.2.6 It may assist the parties, their lawyers and the court if parties were obliged to consider in each case a standard form questionnaire to aid understanding of the architecture of each party's electronic storage systems.

2 Document Disclosure in Commercial Dispute Resolution

2.1 A standard feature of commercial dispute resolution processes in England is some form of compulsory disclosure of documents. The extent of the requirement to disclose documents varies from case to case depending on what is necessary to enable the case to be dealt with justly. Of particular importance in deciding what degree of compulsory disclosure is necessary are the following factors:

2.1.1 Ensuring that the parties are on an equal footing;

2.1.2 Saving expense;

2.1.3 Dealing with the case in ways which are proportionate:

(i) to the amount of money involved;

(ii) to the importance of the case;

(iii) to the complexity of the issues;

(iv) to the financial position of each party; and

2.1.4 Ensuring that the case is dealt with expeditiously and fairly.[3]

2.2 The application of these factors to a particular case may result variously in no order being made for any form of compulsory disclosure (for example in a simple case of contract construction), a "standard disclosure" order or (in larger, more complex cases) a wider disclosure order encompassing all other documents relevant to the issues between the parties or even documents not themselves relevant to issues but which may lead to a train of inquiry enabling a party to advance its own case or damage that of its opponent.[4]

2.3 "Standard disclosure" [5] requires disclosure by a party of:

2.3.1 the documents on which it relies;

2.3.2 the documents which

(i) adversely affect its own case;

(ii) adversely affect another party's case; or

(iii) support another party's case; and

2.3.3 documents required to be disclosed by a relevant practice direction.[6]

2.4 Whatever the ambit of compulsory disclosure required in a particular case, any party may apply for "specific disclosure"[7] of specific documents or classes of documents.

2.5 Disclosure may also take place pursuant to the terms of a pre-action protocol or an order for pre-action disclosure. Such orders are made where disclosure before proceedings have started is desirable in order to dispose fairly of the anticipated proceedings, to assist the dispute to be resolved without proceedings or to save costs.[8]

---

[3] Civil Procedure Rules 1998, Part 1 - the so called "overriding objective".

[4] See Compagnie Financière et Commerciale du Pacifique -v- Peruvian Guano Co (1882) LR 11 QBD 55 (CA).

[5] CPR Part 31.6.

[6] There is as yet no practice direction in force which extends the ambit of standard disclosure in commercial cases.

[7] CPR Part 31.12.

[8] CPR Part 31.16.

2.6 Further, disclosure may be ordered against a person not a party to the proceedings even where that person is not expected to become a party to the proceedings. In such cases the documents of which disclosure is sought must be likely to support the case of the applicant or adversely affect the case of one of the other parties to the proceedings and must be necessary in order to dispose fairly of the claim or to save costs. Disclosure orders against non-parties are, however, limited to specific documents or classes of documents.[9]

3 The Search for Documents

3.1 Whatever form of disclosure is ordered against a party the duty to search for documents within the scope of the order is the same. The search must be a reasonable one having regard to:

3.1.1 The number of documents involved;

3.1.2 The nature and complexity of the proceedings;

3.1.3 The ease and expense of retrieval of any particular document; and

3.1.4 The significance of any document which is likely to be located during the search.

3.2 Details of the search which has been undertaken must be supplied to the other parties so that they have the opportunity to challenge the reasonableness of the search.

4 Recognising Electronic Documents

4.1 The first question is: what is a document? According to the CPR a document is anything on which information of any description is recorded.[10]

4.2 How does this definition apply to documents in electronic form? What is the "document" in electronic form which needs to be described for the purposes of the CPR List of Documents? For example, a laptop computer may contain a number of Word files being electronic versions of letters sent out. If the

[9] CPR Part 31.17. Production of specific documents may also be ordered pursuant to witness summonses or pursuant to letters of request for use in foreign litigation. These forms of compulsory production are, however, not classified as "disclosure" and are outside the scope of this paper.

[10] CPR Part 31.4

letters are printed out and sent, each paper version would be a different "document" for the purposes of the CPR. Are the electronic versions on the laptop also different "documents" or is there a single electronic "document" (being the laptop computer) which contains a number of relevant files (e.g. the electronic versions of the letters)?

4.3 There is minimal authority on the point. Such authority as there is tends to suggest that the "document" is the physical thing on which the information is recorded e.g. the laptop computer, the hard disk, the zip drive, the CD, the printer, the main frame computer and so on.[11] Arguably, parties to litigation should therefore be disclosing such electronic media in these forms (rather than, for example, simply picking out particular files which correspond with our understanding of conventional paper documents such as e-mails or Word files containing letters). Such electronic documents (e.g. laptop computers) will also contain a mass of irrelevant material (such as system files which enable the computers to be interrogated effectively). How are such files to be redacted if the disclosure obligation is to produce the laptop computer as that is the "document"? Is my opponent simply allowed to sit at my computer and interrogate it?

4.4 The definition of "document" in the CPR and its application to electronic media therefore raises a number of difficult issues. This paper considers some of those issues.

5 The Size of the Problem

5.1 Computers have the capacity to retain an astonishing quantity of documentation in electronic form. A 1Mb text file (1,048,576 characters) fills over 200 pages which, if printed out, comprises a stack of paper approximately 1 inch high. On this basis an average PC contains the equivalent information to that of a pile of paper the height of Snowdon. New PCs are capable of holding the equivalent of a pile of printed paper the height of Mount Everest.[12]

[11] See for example, *Derby v Weldon* (No 9) [1991] 1 WLR 652.

[12] This information was provided by Phil Sealey of Deloitte & Touche, London.

5.2 Over 90% of business documents are now created electronically. Email is increasingly used as the primary business communication tool. It has been estimated, for example, that in the year 2000 US office workers sent 7 trillion emails. About 35% of business documents never exist in physical form and that percentage is likely to increase year on year.[13]

5.3 The unguarded use of email as a business communication device is potentially dangerous. Email for many people is equivalent to a "written conversation". It is not perhaps quite as informal as a telephone conversation but certainly not as formal as a fax. But to treat this means of communication any differently from letters or fax communications ignores the fact that email exchanges become part of the business records of the sender and those of the recipients.

5.4 There are numerous examples of email communications that were obviously not intended to be seen by third parties but which ultimately received a far wider audience.[14] This approach to the use of email communication means that electronic documents can be a fruitful source of enquiry. Although "smoking gun" documents are only rarely a feature of complex commercial disputes they are, if they exist, most likely to be in electronic form.[15]

5.5 In the course of preparing a file in electronic form (such as a Word document) many versions of the file are often created. Automatic saving by the computer means that drafts may be retained at various stages of preparation. Text originally inserted in a draft file but later removed may well be retained in electronic form.

5.6 Behind the electronic records of the composition of a particular file, there can even be found a further source of information which is invisible to the eye when the file is made available only in physical form. This so called "metadata" comprises information, for example, on the blind copying of emails, the date and time when documents were inspected by the recipients

[13] These figures were provided by Terry Harrison, business development manager of Legal Document Management Limited, London.

[14] In an email to Monica Lewinsky Linda Tripp wrote: *"Share this sick situation with one of your other friends because, frankly, I'm past nauseated with the whole thing."* Lewinsky replied: *"I will respect that. I would only ask that everything I have shared with you remains between us."*

[15] Electronic documents were of huge importance in the Microsoft litigation. One of the most important pieces of evidence in the Harold Shipman case was the electronic versions of forged physical documents.

and the dates when changes were made to documents in the course of preparation.[16]

6 Categorising Electronic Data

6.1 Electronically held data can be broken down into four categories:

6.1.1 active data;

6.1.2 replicant data;

6.1.3 back up data; and

6.1.4 residual data.

6.2 Active data comprises data directly accessible on the desk top, for example e-filed documents and the inbox and sent items in an email system. Replicant data is that which is automatically created by the desktop computer by way of, for example, a temporary copy of the file made when opening an email attachment, automatic "saves" of draft documents, manual replications resulting from the use of the "undo/redo" features of certain software applications and "recovered" files which become available automatically following a system crash.

6.3 Back up data comprises that which is commonly saved by prudent business organisations on magnetic tapes and which is designed to form part of a business recovery plan in the event of a major incident affecting the business's computer systems. Although accessible the information held in this form is unlikely to be easy to deal with and restoring the data to usable form is likely to require significant resources of time, expertise and cost.

6.4 Residual data is that which is often mistakenly thought of as deleted. The "delete" functions of computer systems are inappositely named. "Deleting" the document, for example an email, simply removes the email from the user's active data. But it positions the document somewhere else in the computer's database and, with appropriate information technology expertise,

[16] Metadata is particularly useful in combatting the growing problem of email forgery. Since emails are normally sent in plain format with no letterhead or signature they can easily be forged by the unscrupulous. But the metadata behind the document may reveal the truth behind the forgery. It can therefore be argued that electronic versions of documents may often be more reliable than their physical counterparts.

can be relocated. Theoretically, a "deleted" email could be overwritten if the computer's hard disk storage was insufficient to contain all data subsequently imported into the computer. But in reality the hard disk capacity of today's computers is such that it will often take many years before "deleted" documents are overwritten. Even when a document is "overwritten" specialist software recovery experts can often restore and retrieve at least part of the document. Even the use of permanent deletion options in response, for example, to the computer prompt: "Do you wish this item to be permanently deleted from your computer's system?" does not in fact remove the information from the disk. Back up data is so easy to preserve that electronic records are now very often retained for periods far longer than physical documents would be retained under a business's document retention policy. "E-document retention policies" are beginning to become fashionable but generally only as a result of warnings from litigation lawyers as to the possible adverse consequences of retaining too much historic data.

7 Searching for Electronic Documents

7.1 It will be apparent that the capacity of computers to generate and to retain very significant volumes of data presents businesses (and their litigation lawyers) with its own problems. Far more information will normally be retained than would ever have been the case if they had been filed in physical form. Indeed, many documents which would previously have been filed in physical form do not exist other than in electronic form. Accordingly, although the apparent size of the disclosure task is magnified by the existence of electronic documents, the capacity to interrogate computers by the use of search terms, at least in relation to the active data, means that a reasonable search of electronically held data is likely to be capable of being carried out very quickly and very efficiently. Indeed, it is possible for a range of business computers to be remotely interrogated, the results of those searches amalgamated on a CD-rom and, using the metadata, a list of relevant files

revealed by those searches created in chronological order at the stroke of a key.[17]

7.2 Yet this ease of interrogation, superficially attractive as it may be, calls into question the boundaries of a reasonable search. By extending the search to the many available sources of electronic data the starting point from which the litigation lawyer needs to conduct a standard disclosure exercise is more burdensome than it would otherwise have been. It would seem to be an abuse of the disclosure process for a business to give wider disclosure than that strictly required simply because this is easier to achieve. Should the burden of reviewing documentation by a human being remain with the party giving disclosure or are there cases in which it is more appropriate for the other party to have the burden of interrogating its opponent's electronic data?[18]

7.3 The Civil Procedure Rules 1998 contain no guidance whatsoever as to the type of search which would be reasonable in the context of electronic data. How, therefore, is a party to litigation to know how far the search for relevant documents should be taken? Is it appropriate to restrict the search to key word searches (recognising that typographical errors in original documents may result in those electronic files being missed by the search when they would not have been missed by a human being)? Is it necessary to go further than searching the active data? Must the party call in IT consultants to search replicant data and back up data? Must the search extend to the buffer memories of computer printers and photocopiers dotted around the office? What about voicemails? Can SMS text messages on company mobile telephones be retrieved? What about handheld devices and mobile telephones? What about archive data which was created on a computer system no longer in use: must old programs and hardware be reinstated?

[17] Systems are now available which are capable of selecting documents for specific custodians, in specified date ranges and on specified subjects from computer databases so that disclosure searches, processing and legal reviews can all be conducted without ever printing to paper.

[18] As far as the authors are aware there has never been a case in which an English court has allowed a party seeking disclosure to interrogate the other party's computer systems but it would arguably be different if the theatre of documentation to be interrogated had already been produced as the result of a search designed to weed out irrelevant documents.

7.4 A number of US courts have grappled with these problems and tried to introduce principles of proportionality into "discovery".[19] There appears to be no uniform approach[20] but an emerging principle seems to be that, if a court considers a request for electronic disclosure to be unreasonable, it may nevertheless be allowed but at the expense of the requesting party. This appears to be the result of a rigid interpretation of the obligation to give discovery of relevant documents whilst at the same time introducing a balancing factor designed to relieve businesses from oppressive discovery requests.

7.5 There are no hard and fast rules that could possibly be devised which would be appropriate in every piece of litigation or, for that matter, even in every piece of commercial litigation.[21]

7.6 It should, it is submitted, be very rare for any disclosure exercise to require recourse to replicant data, back up data or residual data.[22]

8 Practical aspects of exchanging electronic documents

8.1 It is imperative that all parties reach a consensus on how disclosure and inspection of electronic material will take place. In practical terms that consensus should extend to how it should take place, what formats should be used, the nature of the information to be exchanged etc. In order to achieve this it is advisable that the parties and their technical staff should meet as soon as practically possible (and in any event before the case management conference) to agree the appropriate parameters with regard to the electronic disclosure exercise. Before that meeting takes place each party should:

8.1.1 Identify the nature of the information required from their respective clients;

[19] This is the term used in the US.

[20] Although see the recent case of Zubulake -v- UBS Warburg LLC 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y., May 13, 2003) which introduces new guidelines to this area. It is too early for any feedback on how these will be interpreted.

[21] However, it is submitted that, other than in the most exceptional case, a reasonable search for electronic documents should be limited to those documents which are retained in active form or which can readily be recovered. In the latter category, for example, many businesses automatically remove documents from active data after a period of months unless they are specifically e-filed in an active folder. However, such documents can be recovered upon request but only with the expert assistance of IT personnel.

[22] A possible exception might be a fraud case.

8.1.2 Identify the

8.1.3 scope of the search for information in terms of individuals who may hold data and the appropriate time frame when potentially relevant data may have been created;

8.1.4 Identify the range of electronic data to be searched for the information sought;

8.1.5 Identify the nature and scope of the search for data which is reasonably likely to contain relevant information in order to comply with CPR Part 31 and the overriding objective; and

8.1.6 Ensure that clients have been advised and have taken measures to preserve potentially disclosable data from inadvertent alteration or destruction.

8.2 It is important that the dialogue between the parties should extend to the setting of standards for the format of any database to be used for the recording of information that requires exchange. In addition, the media used for exchange should also be agreed with the provision that it should be appropriate for the volume of data exchanged (e.g. if large volumes of data are exchanged, the use of floppy disks would be inappropriate since they are time consuming and costly to produce).

8.3 It may assist the parties at this stage (and the court, if the parties cannot agree and it is required to make an order for disclosure of electronic material at a case management conference) if the parties were obliged to complete a standard form questionnaire aimed at revealing the general nature of the electronic documents held by any party and the architecture of its electronic storage systems. Disputes lawyers already engage routinely in that process in relation to paper documents such that the process is almost instinctive: lawyers generally know where to look to find relevant documents and will know, for instance, to look at the files held by the different departments within their client who may hold relevant files or particular key individuals who may have their own working files and so on. That same thought process needs be applied to electronic media to gain a picture of the electronic

documents that may contain information relevant to proceedings. Set out in the appendix to this paper is our first attempt at such a questionnaire.

9 Storage and Retention

It is necessary to form some view of the extent to which disclosure obligations in litigation would require resort to different categories of electronically held documents before an e-document retention policy can properly be formulated. In general, however, one of the consequences of the almost impossibility of successfully deleting for all purposes electronic documents is that document preservation is unlikely to be a significant issue. That said, the overwhelming likelihood that some form of disclosure will be required in litigation and the availability of interim preservation orders for relevant documents suggests that in formulating such policies thought should be given to the best means of ensuring that business records are retained in readable and searchable form for a minimum period of perhaps 10 years before those documents become more difficult to access.

10 Proportionality

Given the volume of electronic evidence that may exist, applying proportionality from the outset is key when dealing with the exchange of electronic data. There are two aspects to this. If the average PC contains information equivalent to that of a pile of paper the height of Snowdon, are there criteria which parties can use in order to narrow the search to data which is reasonably likely to contain relevant information in order to comply with CPR Part 31 and the overriding objective? In this context it may be reasonable to decide to limit a search to data relating to key personnel only, to limit the search to a particular time frame or to limit the search to data held in particular software applications. Irrelevant file types (e.g. programme and system files) may also be excluded from review. Alternatively, it may be appropriate to employ keyword searching and omit files from review which do not contain the keywords chosen. Such limitations on the searches that are conducted must, of course, be fully explained in the disclosure statement.

Another aspect concerns the categorisation of electronic data into active, replicant, back up and residual data. By its very nature active data will always be the most accessible and cost effective to disclose. Depending on the nature of the case it

would appear that limiting a search to active data or to that data which can readily be recovered would be sufficient.

A recent case in the US[23] has provided guidelines for determining whether data should be treated as accessible or inaccessible for these purposes. The conclusion reached was that "information deemed 'accessible' is stored in a readily usable format... [and] does not need to be restored or otherwise manipulated" (i.e. active data only). However, the fact that data is other than active (this case was dealing with the production of data contained on backup tapes) does not of itself render it inaccessible. The case sets out a three-step analysis to help decide which information should be treated as inaccessible and which party should pay the cost of producing data deemed "inaccessible" according to principles of proportionality. It appears that one of the central questions was: "How important is the sought after evidence in comparison to the cost of production?"

The practical solution to the challenges of electronic disclosure therefore lies, we think, in the following approach:

(1) Ascertain the data sources;

(2) Consider whether limitations should be imposed on active data searches;

(3) Consider whether searches of non-active data should be undertaken and, if so, who should bear the cost;

(4) Discuss with other parties' lawyers before disclosure is given and, if necessary, involve the court; and

(5) Provide a full and transparent disclosure statement.

15 October 2003

[23] Zubulake v. UBS Warburg LLC (supra).

APPENDIX

ELECTRONIC DOCUMENTS QUESTIONNAIRE[24]

The purpose of this questionnaire is to assist each party to consider and explain to the court the architecture of its electronic storage systems, identifying the various electronic media which may contain information relevant to these proceedings and to enable the court to make an appropriate order for the disclosure of such electronic material.

General

1. Please explain, in general terms, the architecture of your electronic storage systems (e.g. in terms of where data may be stored centrally via servers, whether users access central servers and/or create their own files locally).

2. Please identify the networks or servers which you use.

3. Please identify where such networks/servers are physically located.

4. Please explain, in general terms, how individual users gain access to servers and/or mainframes. Do they obtain access via a network , the internet or through other means?

5. How often is information on networked systems backed up and/or archived?

6. On what medium is such backed up information stored?

7. Where are the back up tapes and/or archives stored?

8. Which back up software is used (manufacturer, package and version number(s))?

9. Do you use a data warehouse or on-line back up regime via ISDN, Broadband or other dedicated transmission line?

10. If so, where is the transmitted back-up data stored and by whom?

11. Do you have a disaster-recovery back up?

12. If so:

    (a) on what medium is it stored?

    (b) where are such physical media located?

    (c) what types of disaster recovery computers are used?

---

[24] The authors would like to thank Julian Parker and Edward Wilding of Data Genetics International Limited for their assistance in producing this questionnaire.

(d) which back up software is used?

13. Please list any organisations that may hold data on your behalf, eg ISP providers or scanning and coding bureaux.

14. As a result of the year 2000 upgrade, are there any systems which you have mothballed? If so, please provide details.

Individuals

15. Please identify and list all individuals who you believe may have created electronic documents in your control.

16. In relation to each such individual please answer the following:

(a) Did that person create documents by accessing the network/server?

(b) Did that person create documents which may be stored on a personal computer/laptop/notebook/PDA or any other device? If so, please identify and list the relevant equipment.

(c) Who owns that computer or device?

(d) What equipment did that individual use which may have stored relevant electronic documents (e.g. PC, laptop, notebook, hard drive, PDA, CD-ROMS, DVDs, memory sticks, diskettes, zip drives, printers etc)? Please include equipment that the individual may previously have used but which he/she is not currently using. Please consider all forms of electronic storage media, whether magnetic or optical.

(e) Did that individual produce his/her own back ups? If so:

(i) how often?

(ii) in what media were such back ups stored (e.g. on floppy disc)?

(f) Are there any replaced or removed drives which are no longer in use but which may contain material relevant to these proceedings?