Email discovery - some random thoughts

By Geoff Witham.

Discovery is a well established feature of civil litigation and seems to have grown out of English equity procedures. Whatever its origins it is now a standard procedure in civil litigation in Australia, the United Kingdom and the United States of America.

In broad terms a party gives discovery by serving on the other party or parties a list of documents (which may or may not be verified by affidavit) containing the information prescribed by the rules of the relevant Court. This is the case in both general discovery and (as is now common practice in the Federal Court) discovery by category.

Under the Federal Court Rules the documents which are required to be discovered are:

a. documents on which the party relies;

b. documents that adversely affect the party's own case;

c. documents that adversely affect another party's case; and

d. documents that support another party's case,

of which the party is, after a reasonable search, aware at the time discovery is given and which are or have been in the possession, custody or power of that party. In making a reasonable search, a party may take into account:

1. the nature and complexity of the proceedings;
2. the number of documents involved;
3. the ease and cost of retrieving a document;
4. the significance of any document likely to be found; and
5. any other relevant matter.

The Federal Court Rules define "document" to include any record of information which is a document within the definition in the Dictionary in the Evidence Act and any other material data or information stored or recorded by mechanical or electronic means.

Electronic documents fall within this definition – see Sackville J in *BT (Australasia) Pty Ltd v State of New South Wales & Anor (No. 9)* [1998] 363 FCA:

> *"The starting point is ... that data recorded in electronic form ... is and always has been discoverable, provided it comes within the scope of the discovery orders made from time to time in the proceedings."*

The obligation to give discovery comprehends and extends to all electronic documents and whilst this note concentrates upon discovery of emails much of what is said applies to all electronic documents.

It goes without saying that where a copy of an email, whether sent or received, has been printed out and filed that printed copy will (in the ordinary course) be reviewed for discovery purposes in the process of hard copy file/document review.

One of the first tasks facing a practitioner is to locate emails where they survive in electronic form so that they can be reviewed for relevance and thus discoverability.

Given the advances in technology (which appear to continue at an ever increasing rate) it is possible that documents which are or have been in a party's possession, custody or power are or have been retained in or on file servers, mail servers, application servers, PC hard drives, blackberrys or backup tapes. Consideration should also be given to any records of instant messaging (eg MSN Messenger) and text messages exchanged via mobile telephones.

To conduct a search of the potential storage locations listed (which is indicative and not in any way meant to be exhaustive) to identify emails for review can be a very considerable undertaking – both in terms of cost and time – and will clearly increase with the size of the organisation. Where the practitioner's client is a small one or two person business the task may well be quite manageable but where the client is a large government or private corporation with multiple offices it can appear (and be) quite daunting.

It needs to be recognised that the potential storage locations of emails in electronic form will, by their nature, have varying degrees of accessibility and that has implications for the time and cost involved in accessing and reviewing emails for discovery purposes. The Cresswell Working Party Report of

October 2004 to the UK Commercial Court Users' Committee noted that there are at least five categories of electronically held information with varying degrees of accessibility. The report recognised active or online data, embedded data, replicant data, backup data and residual data.

Active or online data is generally directly accessible and examples include material on hard drives, filed documents and inbox and sent items in an email system.

Embedded data is normally not visible when a document is printed but can be viewed on screen. Word programmes store information about when data files are created, when edited, by whom, and who has accessed them. It includes formulae for spreadsheets and calculations which are programmed into a system.

Replicant data is automatically created by a desktop computer; an automatic backup feature which creates and periodically saves copies of a file as the user works on it. Examples include automatic saves of draft documents, temporary copies of opened email attachments and recovered files automatically available following a computer malfunction.

Backup data is held in a storage system often in the form of a removable optical disk or magnetic tape media. This storage system is not archival in nature and its primary purpose is to preserve information in the case of disaster – it is sometimes referred to as disaster recovery data.

Residual data is deleted from the user's active data and stored elsewhere on the system. Deleting an email removes it from the users active data and it is stored elsewhere on the system and can become fragmented although it is often retrievable with sufficient expertise and time – not to mention cost.

Practitioners will need to consider and decide, on a case by case basis, whether any searches should be conducted of embedded or replicant data to locate emails to be reviewed for relevance and possible discovery.

The location and retrieval of emails from backup data (disaster recovery tapes) can be a very time consuming and expensive exercise. As noted, the purpose of this data is not archival in nature and the techniques used to identify and extract specific documents types are by no means perfect. In some instances accessing the tapes for identification and extraction purposes has been known to corrupt the data and render it useless. In addition the development of technology has meant that the media on which such material is stored can, in cases where the storage is some years old, require hardware and even software which is no longer readily available for the identification and extraction process.

It is important to note that the data stored on backup tapes is only a copy of the material stored on the computer system at the time the backup tape is made. It therefore represents a "snapshot" in time and should not be regarded as a copy of all material which may have been created or passed through the system in question.

Another significant issue regarding backup data is the way in which it is acquired. It is a usual practice for backup tapes to be recycled. Daily, weekly and monthly tapes are made and those tapes (or disks) are reused on a cyclical basis – ie, the tapes are regularly overwritten which has the result of destroying the material already recorded. Practitioners need to be alert to the need to remind/advise clients of their obligation not to destroy discoverable material once legal proceedings become likely and it may be necessary in appropriate cases for the cyclical reuse of backup tapes to cease and additional tapes to be acquired so that material is not destroyed.

The Commercial Litigators' Forum which comprises a number of leading UK dispute resolution law firms noted in its October 2004 discussion paper *Electronic Disclosure* that:

> *"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."*

Many people apparently regard email as a "non document" and this is reflected in the language used in emails and the notably scant, if any, regard for an accurate completion of the subject field in cases where that field is completed. The Forum's discussion paper noted that:

> *"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".*

Once all potential locations of emails have been identified the next task is to gather those which are potentially discoverable for review.

This has the potential to create a whole new set of problems for the practitioner. Emails can be identified by reference to the sender or the recipients but not every email sent or received by a person or group of persons will necessarily relate to the proceedings in question. As noted above, subject fields are not always completed and even when completed may not necessarily reflect the real subject matter of the email – subject fields such as "Your email of 3 June 2005" are common and are utterly useless as a search field to identify emails which may be relevant to the

proceedings. A likely consequence is that a very large number of completely irrelevant emails will need to be reviewed to be sure no relevant document is missed in the discovery review process. Of course that needs to be considered in light of the guidelines of a "reasonable search" noted above.

For practitioners who are engaged in reviewing client documents for discovery it is suggested that an attempt be made to agree with the other parties on the identity and names of individuals as senders or recipients of emails so that identification and review of such materials can be placed within reasonable limits.

The process of identifying and retrieving emails may well require the services of computer system consultants and the process of identification and retrieval can be quite time-consuming which results in a substantial cost to the party making discovery. The subsequent review for relevance and discoverability can also be very time-consuming because of the potential of the large number of irrelevant emails reviewed and this also has the potential for a significant impact on cost.

Whilst government and business generally have benefited greatly from computer systems it seems that a disadvantage is the potential to significantly increase discovery costs over and above the costs which were traditionally associated with review of hard copy materials only. Those costs were themselves not insignificant and in part led the Federal Court to adopt the concept of discovery by category as an alternative to general discovery.

Allowing for the differences between the jurisdictions, the United States appears to have a more mature body of case law and procedures regarding discovery of electronic documents than either Australia or the United Kingdom. This seems to be so especially in relation to the costs associated with that discovery. It seems to be an increasing practice in some US Courts for the party requiring discovery of electronic documents in large and complex cases to be ordered to pay the costs of the location, identification and review of electronic documents rather than the party giving discovery. This is not so in all cases and represents an attempt by those Courts to deal with an issue of real significance to litigants. The practice sometimes extends to a further or final review of where the burden of the discovery cost should finally lie once a matter is finally determined. It is not suggested that this practice should be adopted but is noted as one approach to a real issue that needs to be dealt with.

FURTHER READING

For those interested, the following is suggested as additional reading although it is by no means an exhaustive listing:

1. *BT (Australasia) Pty Ltd v State of New South Wales & Anor (No. 9)* [1998] 363 FCA. Although now some years old this report provides an insight into some of the practical and technological aspects of discovery of electronic documents;
2. Discovery of Electronic Documents – www.computerlaw.com.au/discovery;
3. The Report of a Working Party chaired by the Honourable Mr Justice Cresswell dated 6 October 2004 on Electronic Disclosure. This paper can be accessed from the reports section of the UK Commercial Court website www.hmcourts-service.gov.uk/docs/electronic_disclosure1004.doc;
4. Commercial Litigators Forum Discussion Paper of October 2004 on Electronic Disclosure. This paper can be accessed from www.commerciallitigatorsforum.com; and
5. *Legal Week* article 30 October 2003 "The Future is Electronic". This article can be accessed from the archive section www.legalweek.net.