Discovery of electronic documents

Steve White, White SW Computer Law

Steve is the Principal of White SW Computer Law - Intellectual Property, Information Technology and Telecommunications lawyers. He has over 16 years experience in the IT industry in Australia and overseas. He is an Accredited Specialist in Commercial Litigation is a qualified arbitrator and mediator. Steve is also a MACS grade member of the Australian Computer Society and a Committee member of Victorian Society for Computers and the Law. He is a regular speaker and is published in various Australian and international journals.

INTRODUCTION

Discovery involving electronic documents such as email or software source code poses many issues that do not arise as commonly with traditional paper documents.

These issues include:

- **Working out which documents are discoverable or not:** Having regard to the quantity generated by and the variety of data sources (emails, electronic records etc) used by businesses these days, this has become a much more non-trivial task than in the past.
- **Numerous Copies:** The ease of duplication and the propensity to have multiple copies of data (in various versions for backup and other purposes) leads to multiple intermediate versions of the same document being in existence years after the final document was created. The strict obligation to discover copies of all documents becomes particularly important in this regard.
- **Unforeseen Copies:** Many copies of the document are created by machines in the ordinary course of processing such documents. These documents or the information stored in each different document can be very significant and have real impact on the proceedings. However, without significant technical expertise and understanding of the computer systems involved, these documents are often lost or not discovered.
- **Are the known documents recoverable?** In many cases, backup storage techniques may have utilised superseded hardware and software and the examination of the media can be very difficult when the original equipment is not compatible with modern equipment – for example tape backups have over the years utilised different recording formats and smaller and smaller tape spooling devices and these simply are not usable unless you have a tape reader that is designed to read and house that particular sized tape cartridge or reel.
- **Who has control of the documents?** When off site records are involved, it should be asked in who has possession and control of the data and whether such documentation should be subpoenaed rather than discovered; For example web site logs stored by an Internet Service Provider.
- **Additional Costs:** The abovementioned factors all mean that discovery is a complex and expensive exercise the costs of which could exceed the amount in dispute. Particular consideration needs to be given to the costs involved in ascertaining which documents are discoverable or not and the costs of retrieving data including the time and equipment involved.

This article will examine these issues in more detail in the light of recent case decisions.

PRELIMINARY DISCOVERY OF ELECTRONIC DOCUMENTS

To understand the importance of electronic documents it is useful first to look at its applications in a preliminary discovery scenario.

In matters involving information technology disputes or copying of electronically stored materials, preliminary discovery of electronic documents can play an important role in collecting evidence, identifying potential defendants and causes of action. Often such cases involve incidents in which software or other electronic data is more crucial to the determination of a matter than may be the case in a normal commercial transaction which has been documented electronically.

In the matter of *A2B Telecommunications Pty Ltd v Hinkley & Anor*[1] the plaintiff sought an order pursuant to Rule 32.05[2] that the defendants make discovery of specific documents.

The plaintiff alleged that the first defendant, Adam Hinkley ("Hinkley") had been an employee of the plaintiff from October 1995 until September 1997 and during the course of his employment, had developed source code for certain computer software applications.

The plaintiff further alleged that prior to resigning from the employ of the plaintiff (without notice) and moving to Canada, Hinkley deleted or encrypted all copies of the source code on the computer systems of the plaintiff.

In related proceedings *Hotline Communications Ltd & Ors v Adam Hinkley & Ors*[3], Hotline Communications ("Hotline") obtained in 1998, by way of an Anton Piller Order, copies of source code for various software applications and related materials from Hinkley and other parties. Hotline claimed, amongst other things, that Hinkley had deleted certain source code from computers at Hotline Communications' premises in Canada and had left in similar circumstances to those of his departure from A2B.

A2B sought preliminary discovery of the materials obtained by Hotline by way of the Anton Pillar order to

determine whether the source code developed for Hotline by Hinkley was the same or substantially the same as the product developed by Hinkley during the course of his employment by A2B.

If was found by Warren J that notwithstanding A2B's suspicions, it could not know of any similarity between the respective source code until it had the benefit of inspection of the documents it sought to be discovered.

Following inspection, litigation was subsequently commenced by A2B against Hotline, Hinkley and other parties based upon the similarities found between the source code, the other electronic information which was discovered and the analysis that this made possible.

An application for preliminary discovery need not be for specific documents it may also be used in order to identify a respondent[4]. *London Economics (Aust) Pty Ltd v Frontier Economics Pty Ltd*[5] is an example of a matter in which the applicant sought discovery by certain parties then employed by the respondent, and had been formally employed by the applicant, of materials including, amongst other things, computer programs, data files, computer tapes and CD-Rom disks containing relevant information. The applicant satisfied the court that in compliance with Federal Court Rues O 15A r3 and r6 that it had made reasonable inquiries to elicit the relevant information and its inquiries had been unsuccessful.

Finkelstein J, in following Gobbo J in *G Breschi & Son Pty Ltd V AFT Ltd*[6] found that whilst it was not a legitimate use of O 15A, r3 for parties to be examined about their own involvement, the rule can be used in cases where there are many prospective defendants, none of whom have been sufficiently identified as potential defendants, to ascertain who might be the proper defendant.

Electronic documents may be particularly useful in such discovery because they often contain within the document itself a record of who has accessed, modified or printed the document and the time and date of such use.

Applicants must bear in mind though, that the cost of such electronic discovery may be high and as in this matter, the applicant may be required to pay for the costs associated with discovery.

POST ISSUE DISCOVERY

Post issue discovery was first introduced in nineteenth century English equity procedures and aims to provide the parties access to all of the relevant documentary evidence in each party's possession so as to prevent "ambush" at trial.

The process involves an exchange of lists of documents which are usually verified by an affidavit following which each party may inspect the non-privileged documents set out in the opposing party's list.

Discovery is an invasion of the privacy and confidentiality of litigants but is incorporated into legal procedure because the public interest in ensuring justice is done between parties is considered great enough to outweigh the interest in maintaining confidentiality.

However, discovery is not directed towards assisting a party on a "fishing expedition". Only documents, which relate to the matter in issue, are discoverable, with it being sufficient justification that the document would, or would lead to a train of inquiry which would, either advance one party's case or damage that of his adversary. [7]

The Federal Court Rules O 15, r 15 requires that the court be satisfied that an order for discovery is, at the time when the order is made, necessary in the interests of a fair trial[8]. It is common practice for parties to categorise and limit the documents which they will seek and provide access to. The choice of such categories should be related to the pleadings in the matter to assist in minimising the scope of discovery to a reasonable level.

A party is not compelled to discover a document which would tend to subject him to a penalty and discovery will not be ordered in proceedings which are analogous to proceedings to enforce a penalty[9]. A party may also refuse to produce any document that may tend to bring him into the peril and possibility of being convicted as a criminal[10]This may be useful in cases where electronic documents may provide evidence of criminal activity such as copyright infringement, but seeking to avoid discovery on such a basis may be prejudicial to the party's credibility.

Where a party has been required to give discovery, they are under an ongoing obligation to discover any document not previously discovered and which would be necessary to comply with the requirement[11]. So in cases where further backup tapes are located or data is successfully recovered that was previously unreadable a supplementary affidavit of documents must be prepared and supplied to the other party.

Australian Federal Court

After a directions hearing pursuant to Order 10, a party may unless the court otherwise orders, require any other party to provide discovery[12]. Although there is no express limit on discovery, the Federal Court may limit discovery under Order 15 r3 where appropriate. In cases involving vast quantities of electronic documents, the parties may be able to request that the scope of inquiry in relation to the electronic records be limited to avoid the sometimes great expense of recovering data where there is little chance of useful information being supplied.

"... the process should not be allowed to place upon the litigant any harsher or more oppressive burden than is strictly required for the purpose of securing that justice is done."[13]

CRITICISMS OF DISCOVERY

Common criticisms of discovery include:

- objectives of discovery are not achieved due to discovery being used as a delaying tactic, a fishing

expedition or as a process to add to the other side's litigation costs; and

- when useful, discovery is at too great a cost.

If the costs of complying with orders for discovery are excessive they should be brought to the attention of the court. In cases involving vast quantities of electronic data, accurate estimates of the cost of providing information in a useable form should be determined and where appropriate used to limit the required scope of investigation. If discovery orders are made by consent, there may be no consideration by the court of the reasonableness of discovery, or analysis of the possible costs and benefits of the process.

Discovery ought not be used by litigants as a weapon with the purpose to delay, harass or drive the other party by exhausting their litigation funds or by otherwise forcing an early settlement. Demanding or producing an overwhelming amount of irrelevant documents or withholding documents can impose a high cost as can excessive legal arguments relating to access to documents.

Options for controlling discovery through more intervention by the court include:

- Keeping the level of discovery proportionate to the type of case;
- Encouraging parties to confer and concur on the scope of discovery; and
- Greater use of 'informal discovery' involving the exchange of relevant documents without the need for verification.

Some of the principles relevant to an application for discovery were summarised by Finn J[14] as follows:

- A party does not have an unqualified right to discovery under the Federal Court Rules.
- General discovery will not be ordered as of course, discovery commonly being ordered only in relation to particular issues or defined categories of documents.
- The rules of court do not place on judges the responsibility of determining for the parties which of their respective documents are required to be discovered. Judges have not traditionally assumed such a role.
- Where a proceeding is one for judicial review, discovery in that proceeding is not to be treated otherwise than according to the normal principles applicable in civil proceedings. Nonetheless, the nature of judicial review proceedings is commonly such that either the occasion for making an order will not arise or discovery will only be ordered in relation to a particular issue or issues.
- Whether or when discovery will be ordered depends on the nature of the case and the stage of the proceedings at which the discovery is sought.
- With the rules of court having prescribed the method by which parties can obtain discovery or further discovery, and having regard to the constraints imposed on discovery, it is impermissible to attempt to achieve discovery through resort to the subpoena process.

But these points do not outline the circumstances in which a court will regard an order for discovery as necessary in the interests of a fair trial. However, important considerations must be the nature of the case and the stage of the proceedings at which discovery is sought.

In relation to discovery orders in doubtful cases, Brennan J[15] stated:

"sufficient is shown to ground a suspicion that the party applying for discovery has a good case proof of which is likely to be aided by discovery".

This was contrasted with the case where *"the proceeding is essentially speculative in nature"*.

In matters involving vast quantities of electronic records, the hurdle to get over in relation to showing a party is "likely to be aided by discovery" should perhaps be set a little higher to avoid the situation where one pary is forced to sift through huge amouns of documentation for items which hey contend will be of little assistance to the other parties to the litigation.

Before extensive data recovery is required, the parties should be given the opportunity to depose as to vhat the electronic records are likely to consist of and why these materials are likely to be of little assistance to the other parties.

PROBLEMS ASSOCIATED WITH DISCOVERY OF EMAILS & OTHER ELECTRONIC DOCUMENTS

The Federal Court Rules define the word "document" to include any material data or information stored by mechanical or electronic means[16]. This definition says nothing about whether such electronically stored documents must be in a reacable format or not. As a result, any data stored by the organisation must be considered when providing discovery.

Despite conventional backup strategies that usually result in periodic overwriting of backup media, the possibility that copies of documents may exist dating back several years due to lapses in applying the backup strategy or retention of copies which would normally have been discarded – for example when a backup tape is determined likely to be unreliable it may be stored and not re-used rather than being discarded. This could mean that years of data will need to be reviewed to determine whether it contains any discoverable documents or not.

Usual back up procedures will need to be reviewed during litigation. The obligation not to destroy relevant evidence during litigation needs to be taken into account so that electronic documents that only exist in electronic form on backup tapes are not destroyed by subsequent overwriting.

In the matter of *BT (Australasia) Pty Ltd v State of New South Wales & Anor (No 9*[17]*)* a large amount of discoverable material existed as e-mails, backup tapes and other

electronic documents. BT (Australasia) Pty Ltd ("BT") filed a motion which claimed that Telstra Corporation Ltd ("Telstra") had failed to comply with its discovery obligations in respect of electronic communications such as e-mails and other electronic documents and had failed to take appropriate steps to prevent the destruction of discoverable documents, including documents in electronic form.

In this matter, Telstra was found to have backup tapes dating back several years despite standard procedures being in place that would normally prevent such long term storage by overwriting data tapes. In his judgment, Sackville J stated that "*...I do not think that technical sophistication is a prerequisite to a litigant or its advisors making inquiries to ascertain whether discoverable electronic communications or documents have been recorded and retained in a retrievable form* " It would seem that the excuse that retrieval and reviewing stored data is difficult and time consuming will not be accepted by the court.

A similar stance was taken by Mansfield J in *NT Power Generation Pty Ltd v Power & Water Authority.*[18] Here the respondents sought an order that the discovery of e-mail communications be limited to discovery of e-mail communications which, since the order for discovery was made, have existed in hard copy form. His Honour was not persuaded that in the interest of justice, the respondents ought be excused from giving discovery of e-mail communications retained only electronically not withstanding the time, expense and effort involved in doing so.

Given that the court is quite comfortable with ordering the wide scale review of e-mail correspondence, what implications might this have in relation to, for example employers' obligations in relation to employees' privacy?

There have been several incidents, particularly in the US, involving employer access to employee e-mail files. Employees more and more commonly send "personal" messages by e-mail rather than communicating by telephone or face to face which means there are written records of statements that once would never have been recorded and there is common unfounded assumption is that anything sent by e-mail is private.

Although there is undoubtedly an expectation that an employee's e-mail will be confidential most computer systems are structured in a way that will allow access to any stored data. Could an employer use indiscreet e-mails located during the provision of discovery to, for example, dismiss an employee if the messages would not have otherwise been read?

Employers should consider consultation with employees in relation to e-mail usage and monitoring and the implementation of well-publicised and understood policies.

Employees should be briefed so as to inform them of the backup and storage of data. In most computer systems, "deleting" an e-mail does not totally remove the document, but often merely makes it more difficult to retrieve. Employees should be warned not to expect privacy within the email system, that even "deleted" e-mail may be retrieved and that the company may read any messages. Companies with international operations may need to consider their privacy obligations, particularly in the EU and alert the court to the fact that orders for discovery may lead to breaches of such obligations.

The rules governing the use of email, particularly to external parties should be carefully considered as it is common for e-mail correspondence to be less carefully worded than other forms of correspondence, particularly when it is not proof read before being sent. Employers should also consider the use of disclaimers or limitations on the use of email as there is a tendency for e-mail messages to reflect the often preliminary thoughts or ideas of an employee that may not have been reviewed by the employer, yet e-mail may be construed by the court to reflect the employer's view.

Once a policy has been developed in relation to the use and storage of email and other electronic documents, it is important for management to liaise with the information system managers in relation to backup procedures. It is commonly considered that backup information should be saved for long periods with the view that "longer is better". Particularly if an organisation is in a litigation prone industry, there should be established procedures to delete electronically stored documents from the backup media.

Of course such procedures need to be implemented based on the assumption that the organisation has adequate records of documentation that would be of assistance to it in the course of litigation, otherwise stored. The removal of backed up materials should be done in a systematic way to reduce the likelihood of a heavy burden in relation to discovery being forced upon the organisation rather than from the view of destroying all possibly incriminating evidence.

Should there be a requirement for the term of retention being at least as long as any applicable statute of limitations or regulatory review period? At the moment, there are no such restrictions in Australia specifically directed toward electronic documents, but this may be an area of change in the future as more and more documents are stored only in electronic form.

However, having a backup and purging policy in place is only effective if the policy is implemented correctly – for example, have you considered what is done with discarded backup tapes? Are they simply thrown in the rubbish or is an effort made to physically destroy the media so that any stored data is irretrievable. Similarly, storage media that has been overwritten may be able to be manipulated in order to recover the earlier recorded material if the time and effort is justified.

Internal housekeeping will reduce the burden of discovery, but it does not mean that copies of electronic documents will not be stored by, for example, the recipient of email messages, on disks and backup tapes of intermediate external IT systems