e-Discovery

Gillian Coumbe, Barrister, Auckland

identifies a new challenge for commercial litigators

The use of electronic evidence in civil litigation is rapidly increasing. In the US, for example, its use has been described as "explosive" and a "tsunami". ("Digital Discovery and Electronic Evidence" Annual Meeting of ABA, August 5, 2001) Today some 97 per cent of business documents are created electronically and more than 35 per cent never reach paper. These documents are not just emails but spreadsheets, memos, reports, presentations – any type of document created electronically. They include documents that may have been deleted and now reside only on backup tapes or other media.

Electronic data is now a routine part of discovery in modern commercial litigation. For lawyers, understanding electronic discovery, or "e-discovery", is now essential. In its simplest terms electronic discovery refers to the retrieval of materials originating from the computer. In practice, though, true electronic discovery extends beyond the origin of the computer files to encompass the analysis, gathering, processing, review and production of discovery materials in electronic format from start to finish.

HIGH COURT RULES

If parties maintain electronic data and communications for business purposes, they will be obliged to produce that information in discovery. Information which is stored, used or transmitted in electronic form should be available through discovery with the same openness as traditional forms. In *S P Bates & Associates Ltd v Woolworths (New Zealand) Ltd* (HC Auckland, CL15/02, 15 November 2002) Salmon J stated, at 3:

> It is, of course, clear that computer records, no matter how difficult they are to access, are *prima facie* discoverable if they are relevant in any way to the issues raised in the pleadings. In that respect there is no difference between hard copy records and computer records.

The High Court Rules do not deal expressly with electronic discovery other than in the definition of "document" in R 3 which includes:

> (b) Any information recorded or stored by means of any tape-recorder, computer or other device; and any material subsequently derived from information so recorded or stored.

The Rules Committee has recently released a Consultation Paper setting out its proposed changes to the discovery provisions. The draft does not make any change to R 3(b). The Rules Committee has stated that in its view the discovery of electronic data is covered by the draft new general discovery rules, but has sought comment on whether or not any specific rules are needed to cater for "e-discovery". It will be suggested in this paper that rules dealing expressly with electronic discovery would be desirable, particularly to regulate access to the other party's database and cost shifting where the retrieval of inaccessible data, such as deleted emails, is sought.

DELETED EMAILS: MODERN SMOKING GUNS

Emails are proving to be a rich source of trial evidence. That is largely because emails are uniquely suited for the most candid and unguarded communications. "It is often shot out of the computer without a second of reflection and with an apparent mentality that it somehow has a different impact than a formal company memorandum or letter: Schlosser, "E-mail E-merging E-normously in litigation", *The Nassau Lawyer*, April 2001.

In the US there have been many headlines about devastating "smoking gun" emails uncovered in legal proceedings. For example, email messages dashed off years ago by the Microsoft Chairman, Bill Gates, and his top executives, had a dramatic impact upon the antitrust case against Microsoft. This led to a comment in *The New York Times;* 11 Nov 1998, p 10, in an article headed "Corporate Delete Keys Busy as E-mail Turns up in Court":

> Never mind monopoly power in the marketplace; the real lesson corporate America is taking away from the Microsoft antitrust trial is that old email can be a minefield of legal liability, not to mention a source of public embarrassment.

The London *Times* reported on 19 August 2003, in an article about the Hutton Inquiry headed "E-mails turn up heat on No 10", that email messages sent by Tony Blair's closest Downing Street aides "threatened to blow a hole yesterday" in Downing Street's insistence that it had not "sexed up" the Iraq weapons dossier, nor "turned the screw" on David Kelly.

Hitting the "delete" key does not mean that an email has been eradicated forever. Computer forensics experts are able to retrieve deleted emails and other documents. Whether electronic data is accessible or inaccessible turns largely on the medium on which it is stored. Information deemed "accessible" is stored in a readily usable format. The data does not need to be restored or otherwise manipulated to be usable. "Inaccessible" data on the other hand, is not readily usable. Backup tapes must be restored, fragmented data must be de-fragmented, and erased data must be reconstructed, all before the data is usable. In *Zubulake v UBS Warburg* 2003 US Dist LEXIS 7939 (SDNY 13 May 2003), the Court noted that the literature on electronic data storage recognises five categories of electronic data, listed in order from most accessible to least accessible. These are as follows:

- *Active online data*: data in an "active" stage and available for access as it is created, eg hard drives or active network servers.

- *Near-line data*: current data typically on removable media, with multiple read/write devices used to store and retrieve records, eg optical disks or magnetic tapes, stored on site.
- *Offline storage/archives*: current data on removable media that have been placed in storage. Traditionally used for disaster recovery or for records considered "archival" in that their likelihood of retrieval is minimal. Storage is on magnetic tapes.
- *Database components on backup tapes*: data not organised for retrieval of individual documents or files, because the organisation of the data mirrors the computer structure, not the human records management structure, eg individual emails or individual items of accounting data such as an invoice.
- *Erased or damaged data*: data tagged for deletion by a computer user, but which may still exist somewhere on the free space of the computer until it is overwritten by new data. Significant efforts are required to access this data.

The Court in *Zubulake* deemed that the first three categories were typically accessible, and the last two typically inaccessible. Deleted emails can be recovered from backup tapes and, using forensic software, from the hard drive.

Solicitors need to be proactive in advising clients of the potential discoverability of current and deleted emails, and of the need for clients to educate employees within their organisations to be more guarded and less uninhibited in their email correspondence.

MANAGING e-DISCOVERY

Discovery involving electronic documents poses many issues that do not arise with traditional paper documents. The importance of solicitors managing electronic discovery well has been emphasised by a number of commentators: Peter Naismith, "Discovery of Electronic Evidence", (2002) 24(6) *Bulletin* 12; Steve White, "Discovery of Electronic Documents", (2001) 44 *Computers & Law*, 46. It is advisable to document the steps taken, as part of an electronic discovery plan. This may assist the solicitor in responding to any subsequent order for further discovery made against the client. A prudent approach to electronic discovery should include a number of steps.

Before initiating discovery, inquire as to the nature of the client's computer system. It may be useful to go past management and straight to the "techies". "Management usually doesn't know much, but if you get to the computer geeks you will find all sorts of things management would probably tell you weren't possible – because of simple ignorance of what their technology can do": Krause, "Discovery Channels", *ABA Journal*, July 2002, 49.

The key persons in the client's organisations who may have relevant information in their electronic possession need to be identified. Search of electronic data should not be confined to desk top PCs but should include:

- laptops;
- home computers;
- computers of PAs/secretaries/staff;
- palmtop devices;
- network file servers;
- archival storage systems, including memory sticks; and even
- mobile phones.

Find out details of the clients' backup procedures and of any existing document retention and destruction policy.

Ensure that the client is aware of its obligation to avoid destroying relevant documents. Preservation can be important owing to the ease with which information stored in electronic form can be overwritten or otherwise altered. The client's existing document retention policy and backup procedures may need to be modified or suspended once the client is on notice of litigation.

In *BT (Australasia) Pty Ltd v State of New South Wales (No 9)* [1998] 363 FCA (9 April 1998, Sackville J) BT sought orders for further discovery, complaining that Telstra had shredded relevant documents and deleted or erased backup tapes containing emails and other electronic documents. The Court found that prior to the hearing of BT's application Telstra had done nothing to prevent the overriding of its backup tapes. Telstra backed up the information on its servers on to magnetic tapes on a regular basis. The tapes were periodically revised and this caused the loss of the information stored. The Court accepted, however, that that was due not to a deliberate decision to delete discoverable material, but rather a failure to appreciate that its customary procedures needed to be modified to ensure full compliance with its discovery obligations.

Although Telstra was able to rely on its ignorance and the fact that its opponents in other cases had not sought its backup tapes, the Courts are likely to be less indulgent in the future, as the decision in *McCabe v British American Tobacco Australia Services Ltd* [2002] VSC (Eames J, 22 March 2002) illustrates. Eames J held that the defendant and its solicitors had subverted the discovery process through a deliberate strategy designed to deny future litigants such as the plaintiff access to potentially relevant information. The defence was struck out save as to damages. The decision was overturned on appeal: *British American Tobacco Australia Services Ltd v Cowell* [2002] VSCA 197 (6 December 2002), and an application for special leave to appeal to the High Court of Australia was recently declined. The case is, however, a salutary lesson as to how the discovery process can potentially go wrong, with drastic consequences for all involved.

If the other party is likely to have in its possession relevant electronic evidence, it is advisable to write to that party's solicitor and request an undertaking that the backup tapes held by that party will not be revised and that the information stored on them will be preserved. If necessary, a preservation order can be sought.

In *S P Bates v Woolworths,* the plaintiff applied for a preservation order requiring the defendant to copy its computer hard drives. The Court declined the order because discovery was imminent and because the plaintiff had not discharged its onus of demonstrating a real risk of removal or destruction of relevant material. However, Salmon J did express concern that some information had been destroyed in error, and emphasised the need for the defendant's solicitors to properly advise their client as to the need to preserve relevant computer information:

> [8] ... The Court would expect that prior to the discovery process being completed the company's present solicitors will explain in adequate detail ... the full extent of the discovery obligations of the defendant and will take such other steps as are necessary to ensure that the solicitor's responsibilities in relation to discovery are properly fulfilled.

Discuss with the solicitor on the other side his/her client's computer system. It may be necessary to include a computer expert and to find out what computer systems (hardware and software) were in use at the relevant time, the possible locations of relevant information, the capacity of the parties to retrieve that information, and the measures being taken to preserve that information. In other words the solicitor probably needs to ask the other side many of the same questions he or she has already asked his/her own client.

Try to reach agreement with the other side as to the scope of electronic discovery, a feasible timetable for compliance, and details such as the form in which the requested documents should be produced. Krause has suggested that without an agreement even a straightforward request for an archive of a company's emails could become a "confused mess". The *BT (Australasia) Pty Ltd* case, which involved large scale interlocutory disputation, is a striking example of how drawn out the e-discovery process can become without co-operation and agreement.

Where deleted documents such as e-mails are sought, the other side may resist disclosure because of the potential cost and time involved in retrieving the documents – a computer consultant will usually need to be retained and sometimes a forensic expert will be required. In such cases an application for further discovery under R 300 will often need to be made. The Courts, in determining such applications in the context of e-discovery, balance the potential burden (cost, delay etc) against the potential benefit of the additional discovery to the other party and to the conduct of the litigation. In addition, as with other discovery applications, any order is subject to the general requirement in R 312 that it be "necessary" at the time, in the sense of "reasonably necessary" (although that requirement is omitted in the draft new R 300). Some examples include:

- *Idoport Pty Ltd v National Australia Bank Ltd* [2001] NSWSC 435 (22 May 2001). Einstein J stated, at [28]:

  > I accept and acknowledge that it is a difficult question as to the circumstances and occasions when as part of discovery obligations, the Court will oblige a party to proceedings to engage or pay for computer experts to undertake experiments in an attempt to resurrect material which once appeared on a computer or was perceived as still reposing in what is colloquially sometimes referred to as the computer's "deep memory". To my observation, that question and the extent to which the Court would ever oblige a party to take those steps on discovery should be determined on an instant specific basis depending on the particular case, depending on the particular issues, depending on the costs involved, and depending, obviously, on all the particular circumstances.

- *NT Power Generation Pty Ltd v Power & Water Authority* [1999] FCA 1669 (25 November 1999, Mansfield J). There the respondents applied for an order that their discovery of e-mails be limited to discovery of e-mails which existed in hard copy form. The Court accepted that it would impose a substantial burden upon the respondents in terms of time, effort and expense to try and restore deleted e-mails from the backup tapes. However, the Court considered that the interests of justice required that those documents be discovered.

- *BT (Australasia) Pty Ltd v State of New South Wales (No 9)*, above, Telstra was ordered to discover deleted e-mails and attachments recorded on backup tapes. The Court did not accept Telstra's argument that the benefit of the additional discovery was too uncertain to warrant the burden of trawling through vast amounts of data recorded on the backup tapes.

- *Invensys Plc v Load Logic Ltd* (HC Christchurch, CP 73/01, 26 March 2002, Master Venning). The plaintiff sought further discovery of email, including deleted emails. The Court accepted that the retrieval of deleted documents from a computer's "deep memory" may on occasion be required as part of discovery. The Court was not prepared at that stage of the proceeding to require the defendants to go to those lengths but reserved leave for the plaintiffs to reapply.

The question of who should bear the costs of retrieving the electronic information becomes important. That issue is dealt with separately below.

Consider whether it is sufficient merely to obtain hard copies of the electronic data discovered by the other side. Occasionally it may be important to obtain access to the other party's database. This raises a raft of further issues, discussed separately below.

COST SHIFTING

In the world of paper discovery, the normal rule is that the producing party bears the financial burden of production. An exception is where an order is made against a non-party under R 299(1) or R 301(1), when the Court has express power to order the applicant to pay the costs of compliance: R 302 (now draft new R 303).

One important issue Courts in the US have been grappling with is how to allocate the costs of e-discovery. Electronic discovery may be a more complex and expensive exercise than paper discovery, especially if discovery of deleted documents is sought and it is necessary to retain a computer forensics expert. The solution adopted by the US Courts has been to consider cost shifting: forcing the requesting party, rather than the producing party, to bear the cost of making discovery. If acting for a party on the receiving end of an application for discovery of "inaccessible" data, solicitors should seek cost shifting on behalf of their clients. The US cases provide some useful guidelines that could be invoked by the New Zealand Courts.

The leading US case is *Zubulake*. The plaintiff employee sued the defendant, her former employer, for damages for gender discrimination and illegal retaliation. She contended that key evidence was located in emails that now existed only on backup tapes and other archived media. UBS estimated that the cost of restoring those emails as approximately US$175,000 exclusive of attorney time in reviewing the emails. The plaintiff moved for an order compelling UBS to produce those emails at its expense.

The Court made the preliminary point that it should not automatically be assumed than an undue burden or expense may arise simply because electronic evidence is involved. The Court observed that this made no sense, and that electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying. The Court considered that the traditional

presumptive allocation of costs should be maintained, and cost shifting could be considered only when electronic discovery imposed an "undue burden or expense" on the responding party. The question whether production of documents was unduly burdensome or expensive turned primarily on whether those documents were kept in an accessible or inaccessible format. Documents stored in database components stored on backup tapes and erased or damaged data, were inaccessible.

Because the documents in issue in *Zubulake* were in an inaccessible form, namely deleted data on backup tapes, cost shifting could be considered. The Court held that the following seven factors were relevant to the cost shifting analysis:

(a) extent to which the request is specifically tailored to discover relevant information;
(b) availability of such information from other sources;
(c) total cost of production, compared to the amount in controversy;
(d) total cost of production, compared to the resources available to each party;
(e) relative ability of each party to control costs and its incentive to do so;
(f) importance of the issues at stake in the litigation; and
(g) relative benefits to the parties of obtaining the information.

UBS was ordered to produce at its own expense documents from a small sampling of the requested backup tapes to determine what data might be found. The Court indicated that it would conduct a cost shifting analysis after reviewing the contents of the sample tapes.

UBS duly submitted relevant information contained on sample backup tapes. In a subsequent decision dated 24 July 2003 (2003 US Dist LEXIS 12643 (SDNY 24 July 2003)) the Court noted that UBS had advised that it had spent a total of $19,000 in restoring information contained on the sample backup tapes, and that it estimated that the total cost of restoration, searching and production of information from all the backup tapes would be $273,649. Of that sum, $165,954 represented the cost of restoration and searching only. UBS asked the Court to shift these costs to the plaintiff.

After applying the seven-factor cost shifting test set out above, the Court ruled that a 75/25 cost sharing split, with UBS bearing the majority costs, would be appropriate. It should be noted that only the costs of restoration and searching were shifted. The Court considered that the responding party should always bear the cost of reviewing and producing electronic data once it has been converted into an accessible form.

The New Zealand Courts could adopt similar guidelines, on a case by case basis. However, there is arguably a need for new rules dealing specifically with this issue.

ACCESS TO THE OTHER PARTY'S DATABASE

The usual practice in New Zealand is for electronic documents to be described in a list of documents in the normal way, and then produced in hard copy form or on CDs containing specific documents or files which have been downloaded. Occasionally, however, a party may seek access to the other party's database, either by requesting a forensic "clone" or copy of the computer hard drive (See Judge David Harvey, *internet.law.nz*, 2003, at 255) or, less commonly, by direct access to its computer system. The need for such access may arise:

- where a party requested or ordered to provide deleted emails or other documents claims that it is unable to retrieve the data. The other party may wish to have its own computer forensic expert undertake that task;
- where the nature of the electronic information is such that it can only be examined in any meaningful way by access to the database;
- where access to "metadata" is required. Metadata establishes potentially important details about who accessed or modified a document and when. There is no metadata on hard copy documents.

If agreement cannot be reached, the appropriate application is one for production and inspection under R 307 and, possibly, R 310 (see draft new RR 310 and 315). The burden is on the applicant to satisfy the Court that it is necessary for disposing fairly of the case. At that point the Court will have to consider, if necessary in the light of expert evidence, what information is or can be made available, how far it is necessary for there to be inspection of the database, or whether the provision of print out or hard copy is sufficient, and what safeguards should be incorporated to avoid damage to the database, to minimise business disruption, and to preserve privilege and confidentiality: *Derby & Co Ltd v Weldon (No 9)* [1991] 2 All ER 901 at 906h-907h. The cost shifting analysis discussed above would also be relevant in this context.

In the United States orders granting access to databases are frequent. For example, in *Playboy Enterprises Inc v Welles*, 60 F Supp. 2d 1050 (SD Cal 1999), the Court allowed discovery of the defendant's hard drive to recover deleted emails and outlined a protocol for production. And in *Simon Property Group LP v mySimon Inc* 194 FRD 639, (SD Ind 2000), the defendant was ordered to produce all home and office computers used by four of the defendant's employees. Such orders are also now being made in New Zealand and Australia. Some examples include:

- *Geddes v New Zealand Dairy Board* (HC Wellington, CP 52/97, 20 December 2001, Master Thomson). Discovery was sought of an electronic version of a computer-modelling software, namely a national herd improvement database. The Court ordered that the programme and software be produced for inspection on a computer operated by the second defendant, subject to a number of conditions and undertakings.
- *Idoport v NAB,* above. The defendants sought an order allowing them to inspect the hard drives of the plaintiff's computers. In an affidavit of documents the plaintiff had deposed, in part II, that it had been unable to retrieve, view, or print any documents stored on the computers. An expert was nominated to be permitted to endeavour to recover the lost data from the computer. The Court so ordered, but subject to being satisfied as to the imposition of stringent conditions to protect the plaintiff, including as to confidentiality, expense and possible loss to the plaintiff.
- *Sony Music Entertainment (Australia) Ltd v University of Tasmania* (2003) 198 ALR 367 (FCA). The applicants sought discovery and inspection from the respondent universities of electronic records stored on backup tapes, CD roms and computer hard drives. The applicants alleged multiple infringements of sound recording copyright. The universities opposed the application

on the basis that the material contained in those electronic formats included a wide range of other irrelevant information which could not be segregated or "masked out" for protection and confidentiality. The Court accepted the evidence of the applicants' computer forensic expert as to the shortcomings of the search methods proposed by the respondents and therefore the need for direct access by the applicants. The Court required strict undertakings and conditions regarding confidentiality.

- *North Holdings Ltd v Rodney District Council.* (HC Auckland, M 1260-PL02, 28 May 2003) Master Lang ruled that plaintiff property developer could have access to the hard drive of a personal computer owned by the son of a Rodney District councillor, in order to retrieve deleted emails lost when the computer hard drive was damaged. Conditions were imposed.

The real problem about one party obtaining access to the other party's database is that privileged or irrelevant material cannot be screened out. Accordingly, if such an order is made access must be regulated and safeguards created by way of conditions and undertakings. Unbridled access and fishing expeditions should not be permitted.

As an example, suppose an application is made seeking inspection of a client's hard drive, the inspection to be undertaken by the other party's computer expert. The client's solicitor should, if possible, insist upon safeguards such as:

- the expert should be required to provide a report to both parties setting out the methodology proposed to be used in copying and reviewing the hard disk, and the process to be adopted in identifying and analysing relevant data. The report should be approved by both parties.
- undertakings should be provided by the expert to the effect that the expert:
  - will not use the material obtained for any purpose other than in connection with the proceeding;
  - will not change or alter the computers or any of their content in taking the copy or "clone" of the hard drive;
  - will only provide to the other party's legal advisers emails or other documents which are or may be relevant to the proceeding (and preferably not until the client has conducted a review in terms of what is relevant or privileged).
- conditions should be imposed such as:
  - copying or "cloning" the hard drive onto a disk should be done after hours so as to minimise disruption to the client's business;
  - if feasible, search of the data should be limited to certain key words or search terms.
  - details of the expert's insurance cover should be provided, together with confirmation that the insurance will protect the client in the event of an error or negligence on the part of the expert;
  - no representative of the other party should be present during the diagnostic work;
  - a representative of the client may be present to ensure the expert does not read any documents that are privileged;
- the other party's solicitors and the expert should give undertakings that in the event that any material is seen which is privileged and/or confidential and/or irrelevant to the discovery process, this will not be disclosed to that party, and that confidentiality and privilege are not deemed to be waived by the client in respect of any such materials.

Nonetheless, there are clearly risks inherent in permitting the other side access to a client's database. It is perhaps akin to allowing the other party simply to trawl through all paper files, whether relevant to the proceeding or not. Solicitors should try to avoid such an order against the client. It is preferable to retain control over the e-discovery process and ensure that any retrieval exercise is conducted by the client's own computer expert. Achieving that will require proper cooperation by the client with requests for electronic discovery (subject to the legitimate benefit/burden and cost shifting considerations discussed above). On the other hand, if the other party is refusing to discover data such as deleted emails, then applying for inspection of its database may well prompt it to undertake the review itself and provide the information wanted.

The Rules Committee should give consideration to introducing new rules addressing the circumstances when inspection of an opponent's database will be permitted, the procedures that should be followed, and the allocation of costs. ❐