The new rules on e-disclosure

Rules on e-disclosure came into force this month. **Ed Sautter** explains the amendments to Practice Direction 31, their impact on disclosure practices, and sees more extensive court dialogue ahead

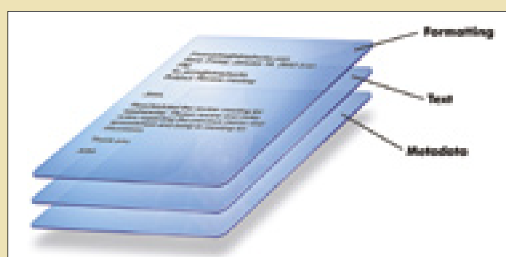
- express definition of "document"—e-communications and metadata
- impact on practice—reasonable search, disclosure lists and statements

In October last year, a report was issued by a working party of the Commercial Court Users Committee chaired by Mr Justice Cresswell, discussing the issues raised by the disclosure of e-mails and other electronic documents. As well as providing a thoughtful analysis of these issues, the working party made recommendations for revisions to the Admiralty and Commercial Courts Guide to deal with electronic disclosure. These revisions were adopted, by way of new paras E3.1A and E4.2A in the guide, on 26 November 2004. The working party also recommended that the Rules Committee consider amending the form of disclosure statement and the relevant practice form (N265) to make clear the extent to which a search has been carried out for electronic documents.

It was anticipated that appropriate amendments would also be made to the relevant CPR practice direction supplementing Part 31 (PD 31). With effect from 1 October 2005, a new para 2A has been added to that practice direction, with corresponding amendments to the form of disclosure statement for standard disclosure set out in the annex to the practice direction and reflected in the amended N265.

Electronic documents: *Practice Direction 31, para 2A.1*

- e-mail and other electronic communications
- word processed documents
- databases
- documents stored on servers and back-up systems
- electronic documents that have been 'deleted'
- metadata—additional information stored and associated with electronic documents



Definition of document

E-documents

Although the fact that electronic records fall within the definition of "document" for the purposes of disclosure under CPR 31 has not been in doubt for some years, the rule made no specific reference to such documents. Paragraph 2A.1 now confirms that the definition of document in r 31.4 is broad and encompasses electronic documents, including "e-mail and other electronic communications, word processed documents and databases". The definition in para 2A.1 also provides that, in addition to documents that are readily accessible from computer systems and other electronic devices and media, it covers documents "stored on servers and back-up systems and electronic documents that have been 'deleted'".

As has become widely appreciated, records that no longer exist—at least in a readily accessible manner—may be found on tapes and other media maintained by organisations for disaster recovery purposes, although their recovery may be by no means cheap or straightforward. Similarly, when an e-mail is deleted, for example, the computer removes the electronic 'pointer' to the relevant file; the file itself remains on the system and hence can be searched for until it is actually overwritten. These latter records are correctly defined as documents. Yet, the extent to which they will be disclosable in any particular case will depend upon the factors determining the extent of a reasonable search.

Metadata

The definition of document is also expressly extended to "additional information stored and associated with electronic documents known as metadata". Metadata comprise information—usually a significant proportion of which is present in the electronic but not the paper form—about the document's properties, such as who edited the document, the date of its creation and the history of prior revisions. While metadata associated with a record may fall within the definition of document, the extent to which it will be disclosable in any particular case will again depend upon the parameters of a reasonable search.

It is interesting to note that both in the draft proposed addition to the Admiralty and Commercial Courts Guide—appended to the *Cresswell Report*—and in the amended para 4 to the guide promulgated on 26 November 2004, it was expressly stated that in most cases metadata were unlikely to be relevant. However, this statement is missing from the new paragraphs to PD 31. It is unclear whether this omission was a conscious one. Yet, as there is no presumption in the practice direction that metadata is unlikely to be relevant in most cases, the parties will have to fall back on the principles defining the extent of a reasonable search in order to determine whether metadata should be disclosed or not.

Cooperation between the parties

Paragraph 2A.2 provides that the parties should, prior to the first case management conference (CMC), discuss issues that may arise regarding searches for, and preservation of, electronic documents.

It is interesting to note the specific reference to the obligation to preserve. The ease with which electronic information can be 'deleted' has placed greater emphasis upon the requirement to ensure that potentially relevant records are preserved. This is likely to increase the incidence of so-called 'litigation hold' procedures within organisations. These procedures usually involve the issuing of notices requiring the preservation of identified categories of electronic—as well as physical—records. The notices are addressed to all those who may hold, or exercise control over, such records at risk of deletion pursuant to, for instance, a company-wide routine e-mail purging programme.

PD 31 also specifically contemplates the provision of information between the parties, not only about categories of electronic records, systems and devices or media upon which the documents may be held but also document retention policies. This is likely

to cast the spotlight on the adequacy or otherwise of organisations' document retention policies in the context of their disclosure obligations.

Paragraph 2A.3 provides that the parties should co-operate at an early stage as to the format of inspection, with the matter being referred to the judge—if possible, at the first CMC—in cases of disagreement. The Department for Constitutional Affairs is still considering draft practice directions submitted by interested user groups, in particular LiST & ALPS, which deal in more detail with the proposed mechanics of exchange of electronic records including those provided by way of inspection. It may be that we will see shortly a more detailed practice direction dealing with the mechanics of electronic inspection.

> *"A helpful rule of thumb may be that the more inaccessible data is, the less likely it is that a party will be ordered to disclose it"*

Reasonable search

Paragraph 2A.4 acknowledges the existence of electronic documents' impact upon the extent of the reasonable search required by r 31.7. It sets out the four familiar criteria determining the reasonableness of a search which are set out in r 31.7(2) (see box, p1620) but criterion (c)—the ease and expense of retrieval of any particular document—is significantly expanded by a series of sub-criteria. These should be studied carefully but, in summary, they include:

(i) The accessibility of electronic documents or data, including e-mails on servers, back-up systems or on storage media which has been superseded by hardware or software developments.

Issues of so-called 'accessibility' have been the subject of considered analysis in various US authorities including the well known *Zubulake v UBS Warburg* decisions. The *Cresswell Report* contains a helpful analysis of the types of data that are likely to be in issue and discusses the US authorities (for instance, see paras 2.18 and 2.21–29). A helpful rule of thumb may be that the more inaccessible data is, the less likely it is that a party will be ordered to disclose it, although the other factors in r 31.7, for instance the importance of the particular document(s) to the issues in the case, are clearly highly relevant to that analysis.

Illustration: David Humphries

(ii) The location of the relevant electronic data and the servers or systems upon which it is held.
(iii) The likelihood of locating that data.
(iv) The cost of recovering it.

A factor to be borne in mind in this context is the flexibility that the court has, under r 44, in exercising its powers to make orders as to costs. So-called "cost shifting" orders have been made in the US and are discussed in the *Cresswell Report* (paras 2.27–29). Consequently, a court may require a party to search for—and if located, disclose—electronic records which are not readily accessible or are accessible only at significant cost, but order the party seeking such disclosure to pay the costs of that exercise.

(v) The cost of disclosing and providing inspection of it.
(vi) The likelihood that it will be materially altered in the course of the above process.

Paragraph 2A.5 recognises that it may be reasonable to search for electronic documents by means of key word searches—agreed as far as possible between the parties—even where it would not be reasonable to conduct a full review of each and every document on a particular database. In practice, key word searches are often the means by which electronic records—in particular e-mails—are located or filtered. The nature and extent of such key word searches are likely to be part of the disclosure statement.

What the practice direction does not replicate from the guide is para E4.2A of the latter, which provides that where an application is made for specific disclosure, the party from whom disclosure is sought should provide information as to the factors discussed above and its document retention policy, to the extent that it is relevant. Although not expressly mentioned in the practice direction, such information is likely to be relevant to any such application.

Duty of search: CPR 31.7

Factors relevant in deciding the reasonableness of a search include the following:
(a) the number of documents involved;
(b) the nature and complexity of the proceedings;
(c) the ease and expense of retrieval of any particular document; and
(d) the significance of any document which is likely to be located during the search.

Disclosure statement

The form of disclosure statement, in an annex to the practice direction, is amended by the addition of a new para 4. These amendments are reflected in the practice form N265. The new section deals specifically with electronic documents and, in respect of searches that were made, requires the following statement; "I carried out a search for electronic documents contained in or created by the following: [list what was searched and extent of search]." Accordingly it is for the disclosing party to identify the types of record and locations that were the subject of the search.

In addition and potentially more significant, is the rather more specific statement now required as to the searches that have not been made for electronic documents. As with paper records, there is a statement that documents created before a particular date were not searched for. The statement then goes on to set out two lists of documents and media upon which electronic documents are stored, and in form N265 each item listed has a box to be marked as appropriate, indicating whether searches were or were not made in respect of that particular type of document.

The lists are as follows. Documents contained on or created by the claimant's/defendant's:

- PCs;
- portable data storage media;
- databases;
- servers;
- back-up tapes;
- off-site storage;
- mobile phones;
- laptops;
- notebooks;
- handheld devices; and
- PDA devices.

Documents contained on or created by the claimant's/defendant's:

- mail files;
- document files;
- calendar files;
- web-based applications;
- spreadsheet files; and
- graphic and presentation files.

These lists are extensive. Various items overlap and there may be some confusion as to meaning of "created by" in the different contexts in which that phrase is used. However, the overall effect is to oblige the disclosing party to indicate the records and locations on that detailed list in respect of which searches were not undertaken.

In practice, a more sophisticated response may be likely where, for instance, certain files or applications have been searched in respect of certain specific personnel but not others.

Finally, the disclosure statement now also requires a statement that searches were not undertaken other than by reference to "the following key word(s)/concepts". This part can be deleted if the search was not confined to specific key words or concepts. However, in many cases, given the potentially huge amount of data to be reviewed, it is likely that key words or concepts will be used in the search. These could include the names of relevant personnel involved in the matter leading to the dispute, and, in appropriate cases, the name (or other indicator) of the transaction or project to which the dispute relates.

Impact on practice

It is clear that the obligation, in the disclosure statement, to provide this potentially extensive detail concerning searches for electronic records that were, or were not, made will encourage extensive dialogue—or controversy, depending upon one's point of view—between the parties. It increases the likelihood that the adequacy of disclosure lists, and accompanying disclosure statements, will be challenged and will lead to arguments, and most likely court applications, concerning the reasonableness and proportionality of searches for electronic documents. One way in which controversy may be avoided is for the parties to conduct—as the rules clearly prescribe—detailed discussions at an early stage as to the extent of the searches that they intend to make. Indeed, it may be prudent for the disclosing party, where it perceives areas of possible controversy which will be highlighted by the matters which it is obliged to set out in its disclosure statement, to engage in dialogue with the other side at an early stage and, if possible, reach agreement or, if that proves impossible, seek court guidance in respect of the searches it intends to undertake.

It is noteworthy that in the US last month, amended civil rules for e-discovery were approved by the Judicial Conference and sent to the Supreme Court. These amendments bear many similarities to the rules discussed above and the parallel development of the two sets of provisions will no doubt be observed with interest.

Ed Sautter is a partner in the litigation & dispute resolution group of Mayer, Brown, Rowe & Maw LLP in London