Communications Law

2007

E-disclosure

Justin Byrne

Subject: Civil procedure. **Other related subjects:** Information technology

Keywords: Electronic disclosure; Electronic documents

*Comms. L. 83 Introduction

Following the issue of a report by a working party of the Commercial Court Users Committee (the Cresswell Report), new provisions were introduced on October 1, 2005 into Practice Direction 31 (' PD 31') of the Civil Procedure Rules (' CPR') in relation to the duties of parties to litigation to search for and preserve electronic documents (' e-documents'). The amendments were necessary because of the ever-increasing importance of electronic communication. Studies suggest that upwards of 90 per cent of all business communications are now created electronically and between 35 per cent and 70 per cent of those communications are never rendered into physical form.[1]

These duties are themselves not new as e-documents have always fallen with the ambit of the meaning of a ' document' in CPR Part 31.4. However, the new paragraph headed ' Electronic Disclosure' inserted into PD 31 has explicitly reaffirmed the meaning of the term ' document.' It makes clear that the term includes e-mail and other electronic communications, word processed documents and databases.[2] In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition also covers those documents that are stored on servers and back-up systems and electronic documents that have been deleted (although often not erased from the computer's storage system).[3] It also includes additional and historical information stored and associated with electronic documents referred to as ' metadata.' [4]

The provisions are quite onerous in that they require the parties to consider many sources of e-documents and provide details to the other side of the categories of electronic documents it has in its control. The disclosure statement (Form N265) has subsequently been amended to deal specifically with the electronic element of disclosure.[5] In addition to the different types of e-document, the supplemental section specifically refers to sources of e-documents such as individuals' laptops and PCs, back-up tapes, servers, mobile phones, PDAs, portable storage media and ' web-based applications.'

It should be noted that the scope of disclosure is not extended and issues such as proportionality, materiality, reasonableness or privilege remain unaffected, and apply similarly to electronic disclosure as they do to paper disclosure. The obligation on the disclosing party is still to provide standard disclosure in compliance with CPR Part 31.6, unless there is a court order to the contrary. The potentially vast number of electronic documents makes the burden of providing standard disclosure, as distinct from a massive dump of electronic documents, extremely onerous.

For this reason and for the traditional pre-Woolf tactical reason of deluging the opposing party with disclosure documents, electronic disclosure given by a party may well exceed the requirements of standard disclosure. This in turn could provoke the receiving party to claim that the other side has failed to provide standard disclosure and to seek an order that they should redo the disclosure process so as to comply with the requirement of CPR 31.6 to disclose ' only' those documents falling within standard disclosure. The courts may, however, be reluctant to make such an order and may choose to impose only a potential cost sanction in respect of the additional costs that can be demonstrated to have been caused by the excessive disclosure. Nonetheless, both sides must give serious consideration to the process of providing disclosure of electronic documents.

Primary source of electronic documents

It is likely that the primary source of e-documents will be ' active data.' Active data is directly

accessible data such as the contents of an email in-box (including archived material) or the hard drive of a PC. Before reviewing emails it is necessary to consider the data protection. This is because of the risk that a review might involve accessing and thereby processing sensitive personal data. The review should not be problematic if the party has a contractual right to inspect all of its employees' emails, if it is in accordance with a court order or if the individual consents. Although this is a grey area, it seems probable that an order to provide disclosure in a piece of litigation would amount to an order that required a review of employees' emails that may fall within standard disclosure. The safest route may be to seek consent. This may not, however, be forthcoming and, in many cases, it will not be desirable for key individuals in a case to review their own emails to establish what will and will not be disclosed. It is likely that the review will need to be conducted by third parties and, therefore, careful consideration needs to be given to the timing and methodology of the review.

Metadata

PD 31 clarifies that an integral part of any electronic document is the metadata associated with it. Metadata, defined as ' data about data' in the US case of *Williams v Sprint/United Mgmt Co* [6], includes information about the document's properties, such as who edited the document, the date of its creation and the history of prior revisions.[7] An e-mail, for example will carry metadata concerning the author, creation date, attachments, and identities of all recipients, including those who only received a cc or bcc.[8] ***Comms. L. 84*** It can also tell you whether that e-mail forms part of a conversational chain.[9]

The availability of metadata is dictated by the properties of the file type. File is the term commonly used to refer to a document when talking about metadata. Depending on the type of application, a single file has the potential to have hundreds of metadata fields.

Metadata can be altered irrevocably by simply opening or copying a document. Therefore, where such data might be relied upon in court, a company should consider engaging document management consultants to obtain a forensic copy and ensure preservation of the data in its entirety rather than attempting to review or copy the documentation themselves.

This is particularly the case in respect of the forensic examination of computers or other equipment. In many instances, even if documents have been deleted, computer forensic experts can find and retrieve the large majority of lost or deleted data by taking an ' image' of the hard drives of the computers concerned while maintaining the integrity of the evidence. This is because, if a document is deleted, only an index to it is removed - the content remains on the computer, albeit for a finite amount of time. Any computers suspected to contain relevant information should cease to be used.

The Admiralty and Commercial Court Guide suggests that ' in most cases metadata is unlikely to be relevant' [10], but this was omitted from PD 31. It is, however, fair to say that in most cases it is unlikely to be relevant. When it is relevant to establish the ' who' and the ' when' or where deception or fraud is alleged, metadata can be a vital tool for searching and analysing documents and will also be disclosable.[11] However, most cases will turn on what a document says on its face, rather than what its history reveals and therefore metadata will only infrequently be strictly disclosable.[12]

Mindful of what a document is, a party should proceed sequentially through the four key stages to giving electronic disclosure. These stages are:

• preservation and collection (often referred to as harvesting);

• processing;

• review; and

• disclosure.

Preservation and collection

PD 31 acknowledges the existence of electronic documents' impact upon the extent of the reasonable search required by CPR Part 31.7.[13] These include but are not limited to:

• the number of documents involved;

• the nature and complexity of the proceedings;

• the ease and expense of retrieval of any particular document; and • the significance of any document likely to be located during the search.

When evaluating the ease and expense of the retrieval (arguably the most important factor) of any particular documents, consideration should also be given to:

• The accessibility of the electronic documents or data taking into account alterations or developments in hardware or software systems used by the disclosing party and/or available systems to enable access to such systems.[14] For example, technology may have advanced such that relevant historical electronic material is incapable of being retrieved economically or at all (such as outdated data back-up tapes which will be expensive to restore). Issues of so-called ‘ accessibility’ have been the subject of considered analysis in various US authorities such as the *Zubulake v UBS Warburg* decision.[15] The Creswell Report contains a helpful analysis of the types of data that are likely to be in issue and discusses the US authorities.

• The location of relevant electronic documents - for example, persons accessing data may be in London but the data may be physically located on servers in the US which would need to be imaged.

• The likelihood of locating relevant data - it is often the case that a company's electronic media, such as back-ups, will contain a myriad of irrelevant information over and above that which relates to the subject matter of the dispute.

The parties should also bear in mind the cost of disclosing and providing inspection of any relevant electronic documents, and the likelihood that e-documents will be materially altered in the course of recovery, disclosure or inspection. The ease with which electronic information can be deleted has placed greater emphasis on the duty to preserve.[16] This has the potential to increase the prevalence of so-called ‘ litigation hold’ procedures within organisations.[17] These procedures usually involve the issuing of notices, addressed to all those who may hold or control identified categories of electronic (as well as physical) documents at risk of deletion, requiring their preservation.

PD 31 recognises that in certain circumstances, it may be reasonable to search for electronic documents by means of key word searches (agreed as far as possible between the parties) where a full review of each and every document would be unreasonable.[18] Details of the key word searches used are likely to be included within the disclosure statement. There may also be other forms of electronic search that may be appropriate in particular circumstances.

It is helpful to apply a five stage test to the first stage of preserving and collecting electronic documents. This will help to establish the reasonableness of a search in the given circumstances of any case:

(1) **What** types/categories of e-documents are going to be required for disclosure? When making a list of the necessary e-documents, it is important to be as prescriptive as possible.

(2) **Who** is likely to have created/sent/received/stored the e-documents? In most instances it will be disproportionate to gather data from across the entire business when only a particular business unit is involved. In practice therefore, this will mean identification of the people most likely to have the documents in their possession (so called ‘ custodians’).

Comms. L. 85 (3) **Where** is the majority of the information stored? Undoubtedly the server will be the primary location. However, there will almost always be further information available on local devices such as PCs/laptops/mobiles/PDAs/memory sticks/Blackberries and so on. It may be appropriate in certain cases to take steps to suspend destruction policies in order to ensure preservation. Retention policies should reveal where any relevant historical material is likely to be stored. The fact that electronic documents may be held on overseas servers is not automatically a reason to exclude them from the scope of a reasonable search.

(4) **When** should the parties focus their search? The application of a date range to a search for electronic documents is an effective way of limiting the volume of documents that need to be collated, processed, reviewed and disclosed.

(5) **How** will the evidence be gathered? This is often dictated by the form in which it currently exists. It is common to use original back-up tapes (that might require restoration) for historic data whereas for current data stored on PC hard drives or servers it is common practice to take ‘ images’ of the data. In straightforward cases, and particularly where there are no issues which require the metadata to be forensically preserved, it is permissible to ask your client for a copy of the data on CD/DVD/external hard drive. In many cases, especially the larger ones, it will be prudent to ask an independent expert to image those storage media identified as potentially holding relevant documents. This will enable the party to prove the

integrity of documents as at the date of the imaging, and thus address any allegations that documents have been tampered with or deleted.

Processing

Given the potentially vast amounts of data that can result from the preservation and collection stage described above, and indeed the Practice Direction amendments to CPR Part 31, it is becoming increasingly common to make use of one of the electronic disclosure management (EDM) systems that are available commercially. A number of processes (such as de-duplication, relevance filters, decryption and date range) can be applied as the data is being uploaded, to filter e-documents for relevance and thereby significantly reduce the volume of gathered data into a more manageable review set.

One of the most common processes is the use of key words, to extract only those documents containing words and phrases identified as relevant to the case. The selection of key words needs very careful thought and the resulting cache of documents needs thorough analysis to establish whether all of the documents retrieved fall within standard disclosure, as it is a virtual certainty that they will not. In short, the process of using key words to harvest documents for disclosure is an additional process to assist in providing standard disclosure rather than an outright replacement of the pre existing processes of manually thoroughly reviewing documents to establish whether they are disclosable.

In smaller cases, data can be processed simply by uploading the contents of a CD/DVD/external hard drive onto a local or central storage area. However, even this will not be necessary in certain instances, and it will be sufficient for the material to remain on the CD/DVD/external hard drive from where it is reviewed.

Review

The review of e-documents is similar in many ways to that of their paper equivalents.[19] A sensible approach is for the data to be divided by custodian so that certain custodians are reviewed by the same member of the review team. The process of reviewing electronic documents and categorising them for relevance to issues in the case (if the data set is contained on a database) is known as ‘ objective coding’ . EDM systems usually contain three predefined categories of documents, ‘ disclosable’ , ‘ irrelevant’ and ‘ privileged.’

Disclosure and inspection

When dealing with electronic disclosure, it is easy to forget that the disclosure process commonly falls into two parts - disclosure by way of list of documents and then inspection of those documents that are not privileged.

Following the exchange of lists, parties must make available to each other for inspection copies of all documents on the list, subject to the following exceptions:

(a) Where the document is no longer in the control of the party who disclosed it.

(b) Where the party disclosing it has the right or duty to withhold inspection, for example privileged documents (the main exception). If a document is no longer confidential, then even if it would otherwise be privileged, privilege cannot be claimed. In particular, care must be taken when using e-mails (and attachments), as the ease with which e-mails can be forwarded and copied means that they can quickly reach a wide audience which may threaten the privileged status of an otherwise privileged document.

(c) Where a party considers it would be disproportionate to the issues in the case to permit inspection of documents within a category or class of document.

Cooperation between the parties

The revised Practice Direction requires the parties to cooperate at an early stage in litigation (and in any event before the first case management conference (CMC)) with regards to issues that may arise relating to how disclosure and inspection of e-documents should occur, what formats should be used and the nature of the information to be exchanged.[20] In order to achieve this, it is advisable for the parties and their technical staff to meet as soon as practically possible to agree the appropriate parameters.

A party is well advised to devote sufficient time and attention to this process, particularly in cases where the disclosure will be substantial. Doing so can help to avoid

subsequent disputes over the adequacy or the excessiveness of the disclosure subsequently provided.

Conclusion

It is clear that the obligation in the disclosure statement, to provide this potentially extensive disclosure of e-documents, should encourage companies to think carefully about their IT and document retention policies and indeed what documents are created.

Although not expressly included in the Practice Direction amendments, the Creswell Report contains a clear warning as to possible cost penalties in relation to e-disclosure:

‘ At the conclusion of the trial (or earlier if appropriate), judges should give separate consideration as to the cost incurred in relation to e-disclosure and who should pay these costs, having regard to the reasonableness and proportionality of the disclosure requested and given, the relevance of the disclosure given or ordered to be given to the issues in the case presented at trial, and the conduct of the parties generally in relation to disclosure.’ [21]

It remains to be seen whether the courts agree with this approach when dealing with the issue of costs. What is clear is that providing disclosure of electronic documents in compliance with standard disclosure is an onerous task that requires detailed advanced preparation, as well as cooperative discussions with one's opponent.

Justin Byrne

Litigation partner, Eversheds LLP, specialising in

IT litigation and arbitration

Comms. L. 2007, 12(3), 83-86

---

1. The Honourable Mr Justice Cresswell, *The Cresswell Report - Electronic Disclosure,* 2004, p 26.
2. Sautter, Ed, ‘ The new rules on e-disclosure,’ 155 NLJ 1618 (2005).
3. Bennet, Philipa, *Electronic disclosure’ ,* ITLT 15 1 (1) (2) (2007).
4. *ibid.*
5. Sautter, Ed, *Op Cit.*
6. 230 FRD 640 (D Kan 2005).
7. Szczech, Andrew, ‘ Disclosing Metadata,’ ITLT 14 6 (2) (2006).
8. Brewer, Jon ‘ Management/IT - Opinion What is metadata and why you should care’ , LS Gaz, 11 May, 13 (2) (2006.)
9. *Ibid.*
10. The Creswell Report, *op cit* p 44.
11. *Ibid.*
12. Brewer, John *op cit.*
13. Sautter, Ed *op cit.*
14. CPR 31PD 2A.4.
15. LLC, 220 F.R.D. 212, 02 Civ. 1243.
16. Sautter, Ed *op cit.*
17. *Ibid.*
18. CPR 31PD 2A.4.
19. *Ibid.*
20. The Cresswell Report, *op cit,* p 43.
21. The Cresswell Report, *op cit,* p 39.