

## Legal Week 2 March 2006

### The Preservation Society

Changes to guidelines on electronic disclosure have raised a number of questions for UK lawyers about the handling and retention of evidence in complex litigation cases. *Michael Taylor* reports.

Changes made in October 2005 to the practice direction to Rule 31 of the Civil Procedure Rules (CPR) have made electronic disclosure a key concern for UK litigators and the companies they represent. In order to comply with the practice direction, litigation teams will need to adopt a much more rigorous approach to the way electronic documents are collected, searched and retrieved. The revised practice direction also clarifies that businesses and their legal advisers have an obligation to consider the availability and relevance of electronic documents at the earliest stages of litigation.

#### **What constitutes a 'document' for the purposes of electronic disclosure?**

CPR Rule 31.4 defines a 'document' broadly as "anything in which information of any description is recorded". The amended practice direction to CPR Rule 31.4 clarifies this definition, extending it to electronic documents that are readily accessible from computer systems and other electronic devices and media (for example, word processing and spreadsheet files, programmes and files used by the computer's operating system).

The practice direction also states, where proportionate and reasonable, that the definition of a document includes data stored on servers and back-up systems and 'deleted' electronic documents (data previously existing on a computer as live data, but that has been deleted by the user or computer system during normal back-up tape recycling).

The practice direction also clarifies that an integral part of any electronic document is its associated metadata. Metadata exists behind the scenes in virtually every electronic document and includes information about who created the document, the date it was created, when it was last modified and more. For example, in an e-mail, metadata would include the 'to', 'from', 'cc', 'bcc' and date/time stamps. The availability of metadata depends on the properties of the file type. Depending on the type of application, a single document has the potential to have hundreds of metadata fields.

Like other forms of electronic evidence, metadata can be altered easily if proper preservation precautions are not taken. In addition, every file and application will have its own set of metadata information unique to that file type. Litigators will need to understand that defining what metadata fields they need to preserve — and eventually produce — is an important step in establishing the scope of the electronic disclosure exercise. In some cases, this may require the assistance of the opposing party or court in clarifying what metadata fields are relevant in the case.

#### **When does the duty to preserve electronic evidence arise?**

A clear standard for determining when the duty to preserve electronic evidence arises has yet to be established in the UK. In *Rockwell Machine v Barrus* [1968], the duty to preserve surfaced when litigation commenced. Meanwhile, *Alliance & Leicester Building Society v Ghahremani* [1992] suggested the duty to preserve arises when the disclosure order is made.

Case law in the US has articulated much clearer preservation obligation standards for litigation in that country and provides that parties have a duty to preserve electronic evidence that they know — or should know — is relevant to the on-going litigation, as demonstrated in *Zubulake v UBS Warburg* [2003].

Case law to help clarify these preservation duties specifically relating to electronic evidence is on now the horizon in the UK. In the interim, the revised CPR practice direction obliges parties to discuss preservation issues prior to the first case management conference (CMC).

The practice direction notes, as part of this discussion, that a party may be required to provide information about:

- categories of electronic documents within its control;
- computer systems, electronic devices and media on which any relevant documents may be held;
- storage systems; and
- document retention policies. If the parties cannot reach an agreement, they may seek assistance from the court.

#### **How should parties plan for disclosure?**

The revised practice direction requires parties to discuss, at the outset of the litigation and prior to the first CMC, a variety of electronic document disclosure issues, including the production format. In complying with this requirement, litigation teams must have thorough knowledge about their clients' IT systems and processes prior to the first CMC.

Litigation teams also need to be aware of the range of electronic document types in their clients' control prior to the first CMC. Cases involving large document sets and multiple data formats may require additional planning in the retrieval, searching, review and production of the document set.

With the assistance of the client and an electronic evidence expert, lawyers should be able to develop an electronic disclosure plan long before the first CMC. The components of an effective plan should incorporate:

- the relevant information;
- potential data locations;
- key individuals likely to possess relevant information;
- internal and external contact information;
- procedural guidelines;
- a documented chain of custody instructions; and
- a summary of anticipated business continuity issues.

Other issues to consider include data collection, data sampling, filtering techniques, delivery method, review procedures, production format, project timeline and cost issues.

### **What is a 'reasonable' search and what is 'proportional'?**

The practice direction to CPR Rule 31.7 requires parties to make 'reasonable' searches for electronic documents. Complying with this directive may mean verifying that all e-mails, documents and spreadsheets within a party's control have been searched. In other words, lawyers may need to comb for relevant evidence located on PCs, servers and back-up systems, removable media — such as CDs, DVDs and USB drives, mobile phones, personal digital assistants, laptops, the web — in the form of extranets, intranets, blogs and so on — and even music players.

Whether a party undertook reasonable measures is based on the volume of documents, the type of case, the accessibility and cost of retrieving the data and the potential relevance of the data at issue.

If a party claims it would be unreasonable to search for a category or class of document, this claim must be made in the disclosure statement and the category or class of document must be identified. Lawyers should be aware that objections to disclosure on the grounds of disproportionate cost may be disregarded in light of a growing number of technological advancements that enable large quantities of electronic and paper-based documents to be collected, filtered, reviewed and produced quickly and cost effectively.

How can lawyers capitalise on technology during the disclosure process? Clearly, not every electronic document is responsive or relevant to a disclosure request. Electronic data-filtering engines can be used to narrow the universe of data down to a smaller, more manageable set.

Common filtering techniques include limiting the universe of data to certain custodians or to documents with specified file attributes — such as keywords, certain document types or whether a file was created or last accessed within a specified date range. Data-filtering typically allows parties to experience a 75% reduction in the number of documents they need to review for production.

Electronic document online repositories represent the most modern document management/review tools, and are gaining momentum in the legal community. An online repository is an internet-based database into which the e-mails and files have been loaded in either a standard file format — such as .tiff images — or the native file format for viewing, categorisation, redaction and searching. These tools result in significant savings of time and cost by allowing reviewers to access their document set remotely via a secure internet connection and review each document file by file.

So with more than two-thirds of UK businesses embroiled in litigation during the past 12 months, lawyers must be aware of their changing obligations under the Civil Procedure Rules. The changes to the practice direction for CPR Rule 31 make it clear that electronic data is included as a matter of course in the definition of a document for disclosure. A comprehensive understanding of this dynamic area of the law will put lawyers in the best position to ensure seamless compliance with electronic disclosure requirements.

*Michael Taylor is a legal consultant at Kroll Ontrack.*