

Legal Week 17 November 2005

Complete disclosure

Legal IT Top 100: From casual e-mails to information on your iPod, electronic data can now be required as court evidence. Jonathon Crook, Jonathan Tardif and Andrew Szczech assess the business implications following recent changes to the Civil Procedure Rules.

Electronic disclosure is set to become a major issue for UK law firms, following the changes to the Practice Direction under Part 31 of the Civil Procedure Rules (CPR) in October. The changes will require a much more rigorous approach to the way electronic documents are created, stored, searched and retrieved. Many of the 'smoking gun' communications that can undermine the strength of a case tend to start life as an electronic document. Casual or instinctive responses by e-mail to a problem with another contracting party, a regulator or even an employee can often be highly significant in the context of formal legal proceedings perhaps months or years down the line. With the scope of electronic disclosure as it now stands, there is an increased likelihood these kinds of documents will see the light of day in court. Regulatory agencies, such as the Financial Services Authority and the Office of Fair Trading, are also becoming increasingly sophisticated and demanding in the information they will seek in the course of an investigation, as well as in the timeframe for its production. Lengthy timescales for collation and review of documents may no longer be feasible when they are stored electronically and can be searched easily.

Electronic documents

The new rules impose increased obligations on businesses to consider the availability and relevance of electronic documents at the earliest stages of litigation. They now expressly refer to documents stored on servers and back-up systems, and will encompass documents that have apparently been 'deleted', but which can be recovered by a forensic expert. An integral part of an electronic document is the metadata stored within it — the data about the document itself, such as the 'to', 'from', 'cc', 'bcc', and date and time stamp on e-mails. It includes concealed information such as hidden columns and formulae in spreadsheets. Most importantly, metadata can reveal the 'who' and the 'when' about document creation, access, printing and editing.

Metadata can be altered irrevocably if the electronic document is handled incorrectly. Even the simple action of clicking onto a document can alter its meta-data.

Scale of the disclosure process

The new regulations have dramatically increased the scale of the disclosure process for a business involved in litigation. The volume and variety of electronic materials produced by businesses continues to increase significantly year-on-year. It has been estimated 93% of corporate documents are created, viewed and stored electronically but 70% of those documents never migrate to paper. The rules state it may be reasonable to search some or all of a party's electronic storage systems — this could mean a complete trawl, not only of the obvious (PCs, servers and back-up systems), but also mobile phones, BlackBerries, laptops, electronic notebooks and even iPods. A party may have to verify that they have searched all mail, document, calendar, spreadsheet, graphic and presentation files and webbased applications.

Proportionality, reasonableness and sanctions for destruction

Electronic documents can be stored and found in numerous places — local hard drives, network servers, back-up tapes and digital devices such as PDAs. Even after a document has been 'deleted', computer forensic experts can usually recover fragments of it, if not the entire document. In this context, much will turn on the principle of proportionality in deciding what constitutes a 'reasonable search' for electronic documents, what electronic documents are or were once within a party's control, and to what extent 'deleted' electronic documents are disclosable.

Factors for determining what would be proportionate and reasonable include balancing the significance of what might be

found against the cost of recovering the evidence in the context of the issues at stake. Lawyers and their clients will no longer find all relevant evidence, or comply with their disclosure obligations, simply by looking through boxes filled with paper documents. Objections to disclosure on the grounds it would be disproportionate and costly to carry out an extensive search can now be criticised — and perhaps penalised — by the court.

The revised Practice Direction to Part 31 requires parties to discuss, at the outset of the litigation and where possible prior to the first case management conference, issues that may arise relating to the disclosure of electronic documents. They should provide information about the categories of electronic documents they possess, the systems, devices and media on which they may be stored, and the storage and document retention arrangements they have made. Parties must also co-operate at an early stage as to the format in which electronic documents will be provided.

It is therefore crucial for lawyers to be familiar with their clients' IT systems and processes for document management. Those who choose to ignore this reality risk overlooking vital evidence and attracting sanctions.

Practical steps

Reviewing back-up tapes is often considered the most fertile source of information in an evidence-gathering exercise. Indeed, in the 'headline' case of *Zubulake v UBS Warburg*, one issue was whether 95 potentially relevant back-up tapes (that is, potentially more than 300 million pages) should be reviewed.

Sophisticated technology now exists for electronic documents to be filtered for relevance and reduced to a manageable review set integrated with paper documents in a single online document repository.

These online databases also provide reviewers with the ability to further search through and filter the documents, place electronic 'post-it' notes and highlight sections on the documents, categorise documents as relevant or privileged and view electronic documents in their native file formats. All reviewers effectively need for an online review is an internet connection. When very large volumes of data need to be reviewed, there is almost no other solution to this type of online repository in terms of both storage capacity and review functionality required.

It may increasingly become the case that parties that could use more sophisticated techniques for managing and disclosing their electronic documents, and fail to do so, will find themselves at a disadvantage in a dispute. As more than two-thirds of UK businesses have been embroiled in litigation during the past year, this is a risk that few can afford to take.

Jonathon Crook is a litigation partner and Jonathan Tardif is a litigation associate at Eversheds. Andrew Szczech is an electronic evidence consultant at electronic and paper-based evidence services provider Kroll Ontrack.