

# Cutting through the fog

While law firms today are more technically savvy than they used to be, practitioners must improve their ability to deal with electronic evidence so that the use of tactical e-disclosure is phased out, says **Martin Baldock**

THE 'EVIDENCE LANDSCAPE' is increasingly challenging, and litigation is increasingly reliant on electronic evidence. Developments in forensic evidence seen in US litigation are beginning to make their way to the UK courts, in particular the 'tactical use of electronic evidence' or its supposed complexity.

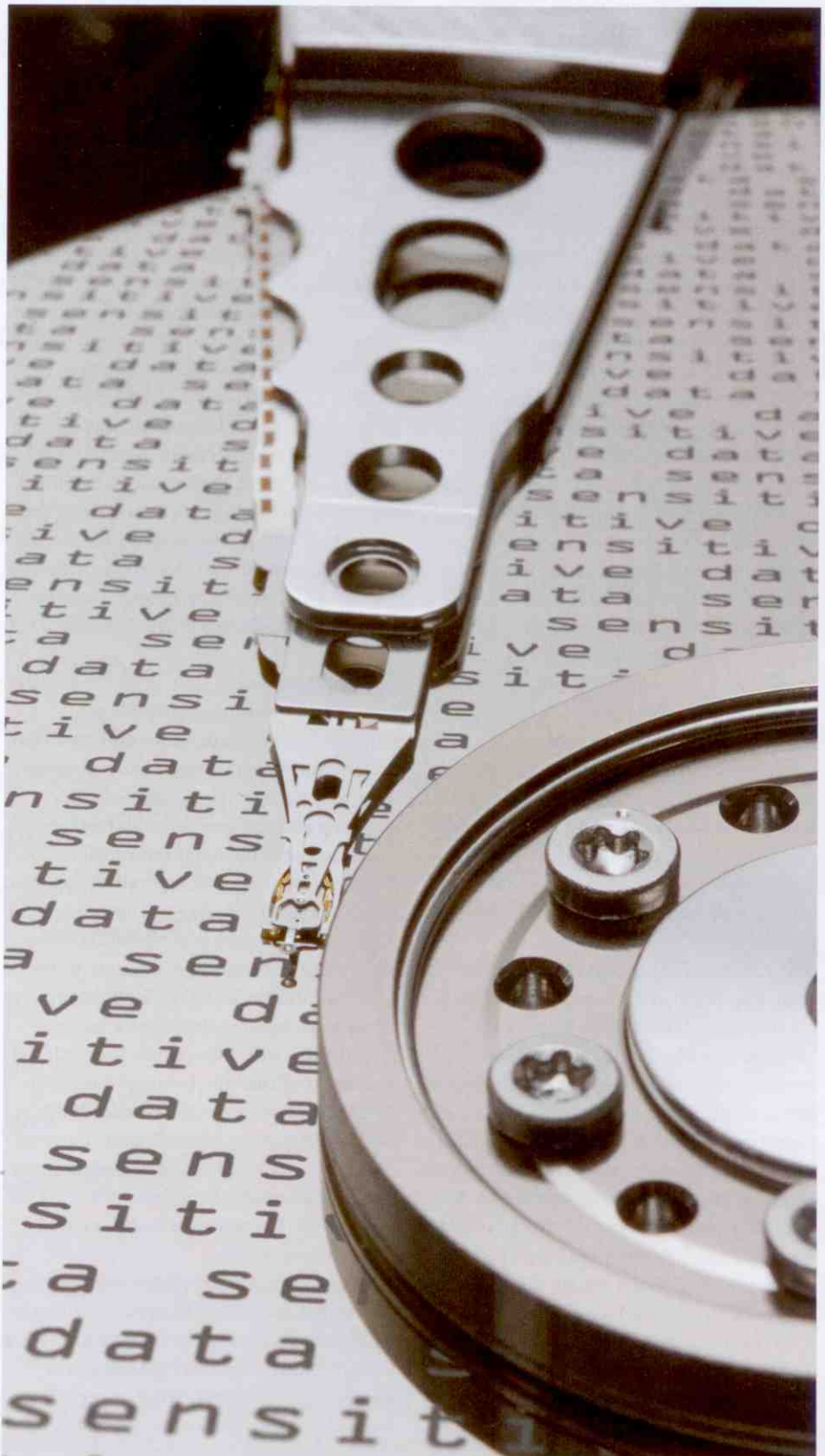
Over the past year there have been several cases where one side attempted to focus on the quality of the other side's e-disclosure (or lack thereof) in an attempt to get their case thrown out. While most lawyers may be familiar with e-disclosure terminology, after all it is far from new in UK litigation, both civil and commercial litigators need to develop their proficiency in assessing their use of electronic evidence and the processes used to gather the evidence. There have been several claims that a particular request is 'far too difficult'; sometimes this even comes from one's own client rather than the other side.

There are four defined phases in any e-disclosure collection. We are now seeing distinct challenges in each. Often these challenges are used as a confusion tactic attached to claims of proportionality.

## Phase 1 – identification

Understanding the evidence landscape is a massive and increasingly complex task, particularly if overseas offices are to be included. It is therefore essential to engage with local IT staff. Often the IT staff feel threatened by the intervention of external specialists and may seek to over-complicate the IT infrastructure. It is of paramount importance to be sensitive to local laws, customs and feelings. A recent engagement we were involved in required data to be collected in several European countries; Germany proved the most difficult to resolve as the works council objected to any data leaving the country. This was despite a court order and took some careful negotiation before the local IT manager was persuaded to co-operate.

Another tactic is to attempt to limit collection and any subsequent disclosure to the topics or custodians that are 'easy' to address. This is an area where the forensic expert



witness can add real value, as the key decision is quite simple in that parties are required to disclose only documents on which they intend to rely and those which adversely affect their own case or which support or adversely affect another party's case. Claims for 'relevant', and 'proportional' (often meaning 'easy') collections, while important, should not be the sole deciding factors; quite often 'easy' collections result in vast amounts of data that is totally irrelevant.

### Phase 2 – preservation and collection

In the past 12 months there has been a slow shift from a limited focus on email and standard office documents to increased awareness that mobile phones, satellite navigation systems, deleted documents and even fragments of overwritten documents need to be considered, extracted and formatted for review by non-technical but legal experts.

This new appetite for previously 'too complicated' evidence has created additional problems. The challenge with these new forms of evidence is how to make them look and behave like an A4 page when they enter the processing stage, as most processing and hosting platforms are designed around the old paper review methods and as such they are expecting something that represents that form factor.

Any formatting or changes made to evidence during the collection phase should be avoided, but sometimes this is simply not possible due to time, resources and other overriding factors. In these cases it is vital to have a properly trained expert who can testify, if necessary, as to what has changed, why it was impossible to avoid this controlled spoliation and what the implications are.

Despite the complexity, and the often unhelpful stance of some data owners, either for or against the case, the following points should be considered by any expert in this field:

- Minimise disruption to client operations. A common mistake is to seize back-up tapes which are then urgently needed for a business continuity issue.
- Be able to prove that the right sources of data were copied forensically and avoiding any spoliation if possible. A full chain of custody including 'hash values' and signed documentation is demonstrable.
- Avoidance of excessive preservation that could significantly increase costs and slow the disclosure process.
- Be able to give assurance to all parties, which could include government bodies and the court, of the integrity and completeness of the forensic collection process.

### Phase 3 – processing, review and analysis

Once the data is collected and preserved the crucial next step is to 'harvest' the user-created data. This is not the same as filtering. Harvesting is yet another area that the unprepared decision maker can fall foul of. Decisions in this area can be as simple as just to exclude the known operating system files, or as complex as only including agreed file types but searching for these by a variety of means such as file header and file signature.

Image files (TIFF, PDFs, jpg etc.) all pose unique challenges. In a recent case one suspect had all emails from a previous system printed out, then scanned and stored on his computer system as TIFF documents. Had the case strategy been to look at just electronic email, these would have all been missed.

Data duplication can sometimes make the original data set seem much larger than it actually is with mobile and static devices often replicating each other. The processing of data from multiple sources must take this into account and a robust de-duplication strategy or identification process must be in place. It is important to remember that probably 80 per cent of the available data will not be important to addressing the issues of the case.

With increasing instances of overseas litigation coming to UK courts, foreign language processing is another avenue of confusion and debate for the decision maker. To engage a review team capable of quickly working through multiple languages is costly; the latest review platforms are introducing 'on the fly' translations which, although machine-based, give the English-speaking reviewer enough of an understanding of the document to make informed decisions.

Historically, if the majority of evidence was believed to be in overwritten data fragments or even deleted files then e-disclosure review platforms would be discounted and the pure computer forensic examiner would be called in. This is no longer a simple decision. Many systems now have the ability to take fragments of overwritten files and convert (or carve) those vital evidence pieces into text documents to upload to the review platform.

As previously mentioned, certain European jurisdictions interpret the European data protection laws in different ways. Another objection often put forward is that data cannot leave a particular jurisdiction and therefore cannot be part of the review and disclosure process. This is no longer a realistic argument. As technology advances,

review platforms can be built or shipped to site anywhere in the world; data doesn't have to leave the country, the review tool can come to the data as mobile processing is now a reality.

### Phase 4 – production and presentation

Both complexity and simplicity claims are tactics used in the final phase as reasons that an e-disclosure process is not viable. Many law firms may have their own in-house system for file review and will only support cases on these systems. The expert witness must be able to work with a variety of systems and be capable of demonstrating a complete audit trail from the initial collection right through to how a document was found to be relevant and thereafter how it was presented to the legal team.

It may be that a particular legal expert will only work with a paper copy of a document set so that has to be tracked to ensure that both electronic and non-electronic reviews are synchronised.

### Trends and tactics

Several companies have now changed the way they manage their electronic documents as a result of litigation in their industry sector, and this trend will continue. It is estimated that one in five businesses have settled lawsuits rather than face the cost of complying with court rules and e-disclosure estimates put forward by suppliers.

The potential conflicts that occur between broad collection, a narrow disclosure, cost and proportionality can be managed by splitting the exercise into stages rather than the US approach to process everything. The expert's role is to help with simple identification, collection and review strategies.

This should be agreed at the Case Management Conference so that all parties know their sources, can discuss them in advance and only involve the court in the case of disagreement.

Judges, counsel and board level decision makers today may still be misled and fall victim to assertions that a piece of evidence either cannot be recovered or that the recovery cost is too high for a particular case. Time is running out for this tactic. The legal community today is more technically savvy than previous generations. Those now growing up with technology will be much wiser about what can or cannot be done, suggesting that the tactical use of e-disclosure in litigation may not be an option for that much longer.

Martin Baldock is vice president and general manager at Stroz Friedberg Limited