

# Digging up data

Retrieval, review, and production of information for disclosure in cross-border litigation are increasingly complex in cyberspace. **Drew Macaulay** analyses the pitfalls and suggests a survival kit

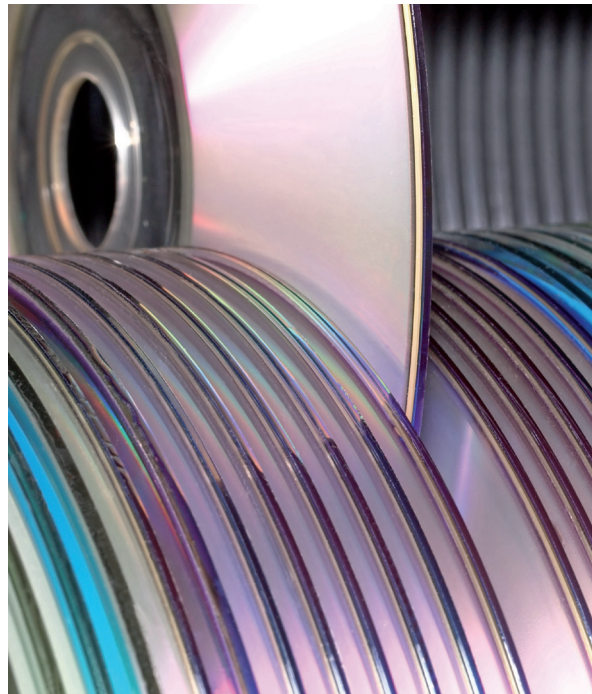
**T**he rise in cross-border trade has been accompanied by an increase in cross-border litigation, arbitration and regulatory investigations. The underlying causes of these disputes are the same as they have always been, but with an added layer of complexity as companies now litigate and respond to regulatory matters in a variety of jurisdictions, with varying legal frameworks and cultural nuances.

When responding to an information request – be it litigation or regulatory investigation – the process frequently necessitates moving large quantities of data between the source, the location where it is to be processed, the location where it is to be reviewed and, its ultimate destination, the party to which it needs to be produced.

## Legal restrictions

The need to move data frequently conflicts with legal restrictions around the movement of personal information at both national and supra-national levels, such as the European Data Privacy Directive or the Japanese Personal Information Act 2003. Common implications of these issues include a need to obtain (and maintain) consent from individuals that their data be collected, that data movement should be restricted to certain jurisdictions and that data may only leave approved jurisdictions if irrelevant personal data has been filtered out and sensitive personal data has been redacted from the document.

Legal instruments concerned with the protection of corporate data such as the French Blocking



## Legal instruments concerned with the protection of corporate data such as the French Blocking Statute may actually criminalise movement of any data

Statute may actually criminalise movement of any data. There are also internal corporate data restrictions where companies responding to information requests have contractual obligations to protect their clients' data, and state data restrictions such as the Law of the People's Republic of China on Guarding State Secrets, where review by the state of certain classes of documents may be required before their movement outside the country of origin.

In all cases the first action to take is to seek advice from local counsel, particularly those with experience of supporting information requests. They will be able to provide practical advice and local assistance with obtaining consent from the employees whose data is required (often termed 'custodians'), guidance as to the local application of data privacy laws, and they may be able to assist with a first level review for privacy prior to data export.

Technological approaches include working with a service provider based in (or capable of travelling to) the country of origin to filter the data to reduce the number of irrelevant documents moved and to review the data remotely.

## Cloud storage

For countries such as France where the Blocking Statute is an issue, those involved could consider using the Hague Convention procedure to obtain requisite permissions for the movement of data, but be warned, document requests will need to be very specific and may take significant time to be approved. For matters where the company has an obligation to retain possession of the data, it is possible to instruct an e-disclosure expert to work on the corporation's premises to process and make available documents for review.

The primary difficulty in many cases is simply locating the data to be collected and reviewed. Owing to the high information transfer speed of modern corporate technology networks, and the increasing use of outsourced or 'cloud' data storage, documents of interest

may be located in a different location (or even country) to the staff who create and use those documents.

Being unable to locate information to be preserved, collected and reviewed will lead to delays and potential inaccuracies in the response to the information request. Outsourced data storage providers may not host the company's data in the same country as the users, may not grant access for independent data collection technicians to collect the data, and may store two or more companies' data on one physical storage device, leading to delays and legal complications around access to an individual company's own data.

## **Bespoke databases**

Other problems commonly encountered involve files that have been created in rare or bespoke applications, which reviewers and opposing parties may not be able to open, bespoke databases and documents in certain languages (for instance, Korean, Mandarin, Japanese) which need special handling to avoid corruption of the content and the metadata of the document, which will ultimately compromise the reliability of any searches undertaken further down the line. This is particularly an issue with, for example, Japanese documents in non-Unicode character encoding.

There are few easy solutions at the time of receiving an information request to the problems of locating potentially relevant data across multiple countries, but a small amount of research and planning in advance of the receipt of an information request can make the process much simpler. At a minimum, identifying where the company stores its data and creating a network map showing the physical locations of storage devices and the classes of information contained therein will increase the speed with which a company is able to

## **Other problems commonly encountered involve files that have been created in rare or bespoke applications, which reviewers and opposing parties may not be able to open**

respond.

Companies using outsourced or cloud data storage should make enquiries with the provider as to the physical locations of the servers that are used to house the company's data, as well as how the company should go about retrieving information from those servers if the need arose and whether data on the servers is limited to that belonging to one business.

For information housed in databases, and files in the languages mentioned earlier, it is best to identify and engage with a provider that has experience of undertaking this type of work. They will understand the challenges and have in place the relevant expertise and technical solutions to get the job done quickly and efficiently.

Local support and sensitivity are the keys to a smooth data collection exercise. It is vital that local management understands the reasons for the exercise and the importance of adhering to planned arrangements. Those managers should have the influence required to communicate that importance to local employees, minimising delays.

It can also be helpful to engage with the local trade unions, particularly in countries such as Germany, where gaining (and maintaining) consent to the data collection and processing is vital, and leveraging custodians' trust in their union representatives, who have a more objective view of the reasons for the process, is likewise beneficial. Local lawyers are often helpful in dealing with negotiations with unions, appearing more independent than company

management.

From a technical perspective, select a data collection vendor that is able to provide staff fluent in the local language(s), and that is able to explain, in non-technical terms, how data is treated after the point of collection. Custodians who understand how the information collected from their machines will be used are more likely to give their consent and less likely to withdraw this consent later on in the project.

An often overlooked point is that some parts of the world have different working weeks and weekends (namely, Sunday to Thursday or Saturday to Wednesday). These differences, as well as religious festivals such as Ramadan, Eid and Diwali should be considered and factored into any data collection plan to avoid delays and additional costs.

## **Risk, delay, cost**

Overall, cross-border information requests present a variety of challenges that, if not considered early in the lifecycle of a matter, have the potential to add significant risk, delays and cost to the process. Some work can be undertaken in advance to mitigate these risks by researching and documenting the nature and locations of data held by a company, and making relevant senior stakeholders in operations and IT departments aware of the input that would be needed from them and their teams should a matter arise.

Once an information request is received, selecting external advisors, such as local counsel and technical e-disclosure consultants, should be based on their experience of working on similar projects, their resources in the relevant jurisdictions, and their flexibility to deal with the changes in scope and focus that are frequent features of many of these matters.

*Drew Macaulay is a director of business development at computer forensics and e-disclosure company First Advantage Litigation Consulting*