

# E-DISCLOSURE: HOW TO ENSURE YOUR EFFORTS ARE EFFECTIVE AND DEFENSIBLE

The changing landscape of e-disclosure presents lawyers and their clients with an ever-growing expanse of pitfalls. Julian Parker of Stroz Friedberg offers some expert guidance.

The new legal landscape encompassing the disclosure of electronically stored information (ESI) is daunting even for those with significant experience. There are many pitfalls to even the most rudimentary collection and review of ESI. The new Practice Directions will simplify matters for all parties.

How they are considered and implemented is key to any successful e-disclosure exercise – mistakes are costly and can lead to accusations of incompetence or deliberate destruction of potential evidence. Here we consider the nature of ESI in relation to some key provisions of the new Practice Directions, to ensure legal advisors achieve the best understanding and best results from e-disclosure under the new regime.

## The data issue

The amount of business documentation has increased exponentially – largely as a result of the speed and efficiency of modern communications and processors. Add to this the extraordinary capacity for electronic storage available and you have a disclosure nightmare. Printing out and reading a client's documentation is no longer an option because of the sheer quantity and time required to read it thoroughly.

Even recently, however, discussing ESI and e-disclosure with some advisors has been difficult. They have been reluctant to undertake detailed e-disclosure exercises, either due to cost, which they deem excessive, or a lack of understanding of what's involved (which in turn leads back to their view on cost). This is what new Practice Directions should address.

These will ensure that parties consider ESI early in the litigation process; ignorance will not be a defence. This is a positive development which will level the e-disclosure playing field. Advisors will become more efficient with e-disclosure practices which in turn will drive down the costs for clients. Also, given the size of the data problem, proportionality remains key – to quote:

*"The purpose of this Practice Direction is to encourage and assist the parties to reach agreement in relation to the*

*disclosure of Electronic Documents in a proportionate and cost-effective manner."* The Practice Directions list general principles governing e-disclosure, among the most important of which, echoing the cost issue, and adding the need for technology to assist the exercise, are:

*"Electronic Documents should be managed efficiently in order to minimise the cost incurred; Technology should be used in order to ensure that document management activities are undertaken efficiently and effectively; Electronic Documents should generally be made available for inspection in a form which allows the party receiving the documents the same ability to access, search, review and display the documents as the party giving disclosure."*

## The main problems with ESI

Some singular issues with ESI impinge on any process related to it, regardless of prevailing laws and directions.

**Size** – clients still ask for documents and emails from a user (often from a single computer) to be loaded into some simple format for searching, which they try to achieve using keywords and phrases. This may still be achievable but now even a single user's electronic documents can run into several thousand items. Email adds disproportionately to the problem with the back-and-forth nature of messages between users and the ease with which senders can copy in great numbers of recipients. The size issue becomes very apparent when multiple users are involved.

**Duplication** – whether intended or not, the back-and-forth of emails presents document reviewers with largely the same set of messages over and over again. Documents are also duplicated by system actions (such as backups), different saved versions exist, and different users also have copies of the same documents or emails.

**Backups** – corporate entities invariably back up their data to a safe location. Data may be held in an easily identifiable manner and in an easy-to-reach location and format, for example a mirror copy of emails saved onto a second server. Or backups may be held offsite (in a third-party storage facility perhaps) and on tape (and therefore

not easily viewed). They may not be well noted, making it hard to determine what backup relates to which user and what time period. Equally, they may duplicate each in large measure. Worst, the backup system used to create the backed up data may no longer be in use with no versions of the tools to open it being easily be found, adding significantly to the time, effort and cost of obtaining data for review.

**Location** – data can be widely spread across several systems and locations. Increasing use cloud of computing facilities to manage corporate data makes this even more problematic as the cloud can be totally dynamic, moving corporate data sets between machines and even between continents to enhance performance and storage capacity.

**Portability** – data can be easily moved with exceptional speed. Data that reside in one jurisdiction in the morning can be moved to another by the afternoon. Modern data transfer mechanisms allow movement of vast quantities of data.

**Ease of destruction and loss** – huge quantities of data can be put beyond reach (as forensic experts we hesitate to say "completely destroyed" – which would entail a much more deliberate act) with a simple click of a mouse. Data can also be overwritten or dropped off the network depending on usage policies and available space.

**Ease of alteration** – not only can specific files be easily altered but key information about the files (metadata) can be changed. Sometimes metadata are unintentionally altered by the process of collecting them for processing and review. This can be highly detrimental to the evidential integrity of an electronic document.

**Type of data** – corporates often hold specific types of data relevant to their industry. These may include custom-made or proprietary systems and software. Such data may be hard to extract from the corporate entity and equally difficult to search.

## Planning the first steps

First consider how and what technology should be used. To quote the Practice Directions:

*"The parties and their legal representatives must, before the first*

*case management conference, discuss the use of technology in the management of Electronic Documents and the conduct of proceedings...*"

There is plenty of quality technology, and experts on hand to advise. Lord Justice Jackson believes judges, solicitors and counsel should develop a much more detailed understanding of available technology and how it functions to be able to manage litigation properly, adding that e-disclosure should form a substantial part of CPD for solicitors and barristers.

The Practice Directions also specify the topics that **must** be discussed before the first case management conference. These form the backbone of e-disclosure, and include:

*"(1) the categories of Electronic Documents within the parties' control, the computer systems, electronic devices and media on which any relevant documents may be held, storage systems and document retention policies;*

*(2) the scope of the reasonable search for Electronic Documents required by rule 31.7;*

*(3) the tools and techniques (if any) which should be considered to reduce the burden and cost of disclosure of Electronic Documents, including –*  
*(a) limiting disclosure of documents or certain categories of documents to particular date ranges, to particular custodians of documents, or to particular types of documents;*  
*(b) use of agreed Keyword Searches;*  
*(c) use of agreed software tools;*  
*(d) methods to be used to identify duplicate documents;"*

The first issue is to identify and collect the data set, aiming to collect the right quantity, from the right places, and put the right amount of that forward for review, so that a proportionate search can be undertaken.

At the earliest possible stage in proceedings the client's advisors should meet with their client's IT function to determine where the key data might be and set in motion a hold on any key data sets (including backups).

From this meeting, the advisors and their team should have a sound understanding of the potential size of the problem – i.e. where the potentially

key data should be and how much there is (often aided by a data map). Also from this point, advisors can ensure that no data are lost – an important provision of the new directions.

While advisors have to ensure they have captured all data sets that may be potentially relevant, the concept of proportionality drives the next stage of the process. Advisors must be careful to balance these first two stages correctly. The temptation to exclude data from the collection (or preservation) too early should be strongly resisted. It is better to collect a wider set of data and end up processing a fraction of them for review, than to collect a narrow set of data, and then have to return later for a further collection, chiefly because the data may have changed (or been lost) in the interim and it is always more expensive to go back a second time.

Now the first limiting qualifications should be applied to the data, such as determining:

- The key likely personalities involved – i.e. the number of users (or "custodians") likely to have key data within their set.
- Is there an appropriate date range that can be applied to the data set? If so, how?
- Is there any specific type of data that can be excluded (for example, proprietary software or specific databases of no relevance)? The discussion here should include whether any deleted data or data otherwise beyond normal reach need to be recovered.

From here a more limited set of data should emerge.

## Data collection

Data must be collected properly. They will be collected in different ways – corporate email can normally be copied from the servers by the client's IT function, and this is evidentially sound for most proceedings. However, if e-disclosure experts are appointed, it is good practice for them oversee this process, liaising with the corporate IT staff so that they can confirm that the process is sound and add weight with an appropriate statement.

Data from PCs and laptops have to be collected differently, and with

specialist assistance. This is normally done by way of a forensic image, from which the key user data are harvested out for processing into the main review data set. There may be other data to consider from backup tapes (which may need specialist help depending on the backup regime used) or mobile devices such as BlackBerry handsets. There may also be proprietary software or databases not designed to be easily copied and searched.

## Culling and de-duplicating

Once the master data set has been assembled, it can be greatly reduced in size by a planned cull of specific data. Ensure a cull does not inadvertently exclude potentially key data. De-duplication is key to reducing the plethora of repeat data (especially in email sets), but be careful. Errors are costly to repair later and can result in chaos at the point of disclosure. The key decision is how to de-duplicate.

## The first searches

The data set should now be ready for advisors to perform their first searches. The initial searches are designed to be a way of gauging what is likely to be the quantifiable amount of data that need proper review rather than a full search for material to disclose.

Keyword searching at this point is more an art than a science. A bad choice can result either in a huge and unmanageable data set, or one that is too narrowly defined which will mean further work later – or worse, claims by opponents that the exercise is flawed. As the Practice Directions note:

*"The injudicious use of Keyword Searches and other automated search techniques –*  
*(1) may result in failure to find important documents which ought to be disclosed, and/or*  
*(2) may find excessive quantities of irrelevant documents, which if disclosed would place an excessive burden in time and cost on the party to whom disclosure is given."*

The new Practice Directions should greatly assist in pointing advisors towards gaining maximum advantage from e-disclosure exercises, enhancing their credibility with both the courts and their clients. **CDR**