Litigation and eDisclosure – What should Lawyers do?

LEAD

This article explores the handling of electronic information in the disclosure element of litigation, a procedure commonly known as eDisclosure.

PRIOR (REQUIRED KNOWLEDGE)

The reader should have an understanding of legal process, and want to understand how using electronically based information differs from paper based disclosure.

AIM

The aim of the piece is to take the reader through the process of eDisclosure, starting with a definition of what it does and does not mean, and then progressing (by means of an industry standard model) through the various stages of the procedure.

INTRODUCTION

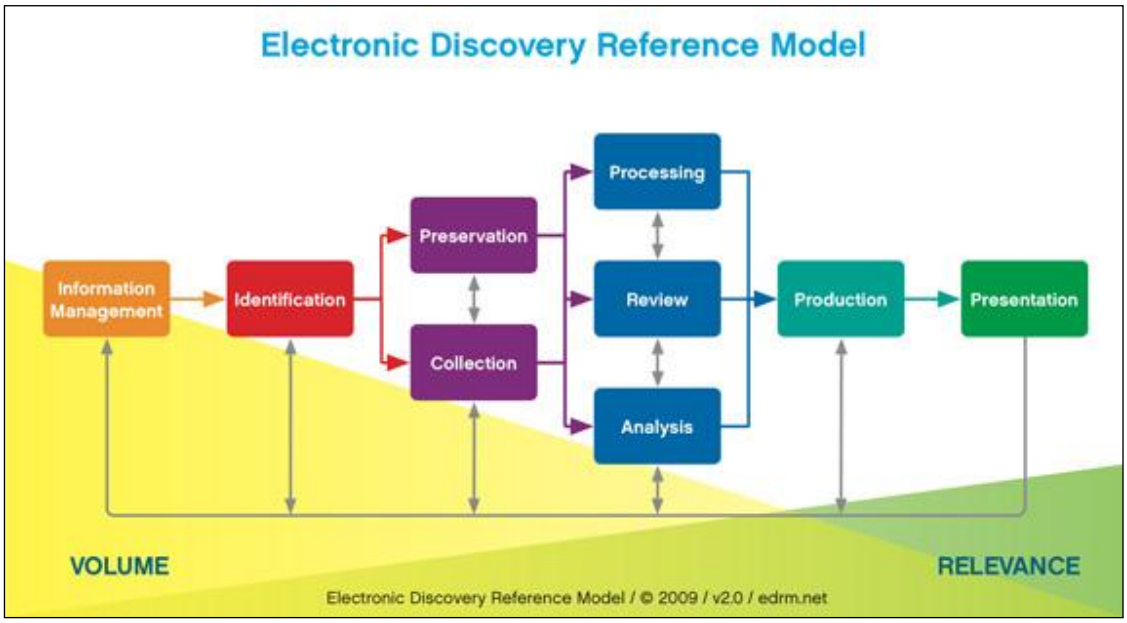
A simplistic definition is that eDisclosure is all about the disclosure of electronic material. However we need to dig a little deeper into that statement of the obvious.

There are two parts to the definition; the words "disclosure" and "electronic material". Let's explore the second one in a little more detail. Electronic information refers to the "stuff" that is within emails, Word documents, Excel spreadsheets and PowerPoint slide shows. This is the level that most readers will need to interact with for eDisclosure. The term also includes databases, social media (Facebook, LinkedIn, Twitter), digital audio such as recorded conversations in deal rooms, support centres et al, images, mobile phones and a host of other increasingly more exotic types/locations. All of this is known as **Electronically Stored Information** or ESI.

The definition of eDisclosure then becomes the process of identifying, collecting, processing, analysing and reviewing ESI for legal proceedings.

For the sake of completeness, eDisclosure is NOT the process of agreeing the electronic media by which information will be transferred. When disclosure was all about transferring images of pieces of paper between legal entities, there used to be discussions on format might be used for the images, and which kinds of physical media could be used to hold the images and their data, be it "floppy disks", tapes or a memory stick. This discussion used to be incorrectly labelled as "eDisclosure", and is mentioned here to dispel any legacy misunderstandings.

As you would expect for a technical process, there is an official model showing the various steps involved in the whole procedure. This is known as the Electronic Discovery Reference Model (EDRM). The model is discussed in great detail at www.edrm.net, but for the purposes of this report the standard graphic used to give an overview of the approach is shown below.



The background in the graphic shows the volume of data decreasing as the various stages are completed, with a corresponding rise in the identification of relevant material. The various processes involved in eDisclosure are shown as discrete boxes with workflows between them. The main use of the model for this review is to provide a "shorthand" to explain the functionality that different software products provide.

For example a company specialising in area of Records Information Management, email archiving and the ability to "freeze" documents within a client environment in order to meet the requirements of disclosure, might state that they "work in the left hand side of the EDRM model". A forensic firm might focus on the purple Preservation and Collection areas, whereas a litigation support software firm might have literature showing them focused on the blue boxes of Processing, Review and Analysis.

The rest of this article goes through each of the "boxes" of the model and look at three things:

- The official description of the individual process/procedure.
- How you as a lawyer might become involved in within this particular process.
- A brief overview of the types of services and/or software products you might need to support you in this process.

INFORMATION MANAGEMENT

This is all about getting your electronic house in order to mitigate risk & expenses should eDiscovery become an issue, from initial creation of electronically stored information through its final disposition.

You might be called upon to assist in terms of providing advice on data retention requirements for a specific industry.

Normally the preserve of the larger consultancy firms working with their clients.

IDENTIFICATION

Locating potential sources of ESI and determining its scope, breadth & depth.

This is the initial stage where the client comes to you and explains their problem. Using a combination of your legal knowledge and their understanding of the organisation they work for,

you should start to get an idea of where the ESI might be located. You might want to incorporate a rough outline of the scope in your initial client care letter, you might be happy with going on what the client tells you (it is their data after all), or you might want to delve a little deeper into what data silo's exist.

In terms of getting help, this is very much a case of selecting the appropriate level of assistance if, or when, it is required.. A good rule of thumb is; do you know enough about the client and their technology to run a "sanity check" over what they are telling you?" If not, you might want to get some professional help to try and uncover any technical issues, before they catch you out downstream.

Some consultancy/forensic organisations specialise in producing something called a "data map". This is NOT a technical document showing all the servers and other bits and pieces that makes up the client's IT infrastructure. Rather it is a written description (possibly with a diagram or two) of where the various data sources are. For example; "*Most of the information is stored on the email servers, but some is on the back-up tapes, and there is a company the main firm took over last year that has got its own IT infrastructure which will need to be examined."*

PRESERVATION

Ensuring that ESI is protected against inappropriate alteration or destruction.

Once you have determined the possible scope of the areas you might (or definitely will) be collecting data from, you need to ensure that the client doesn't delete or damage the ESI in those locations. Again this might be something for your initial engagement letter and you might need technical help. You might cover things like; stopping the re-use of back-up tapes (it can be cheaper to buy a whole new sets of tapes that over-write important evidence), or removing the limits on email in-boxes that cause emails over 60 days old to be deleted, or putting a hold on the re-use of the PC used by the employee that is suing your client.

In terms of software tools, there are very expensive, mainly US based tools, that will preserve ESI across the client's infrastructure. If your client has got this kind of software in place, they are probably involved in serial litigation and you won't be reading this kind of article.

The key area that causes problems is when there is a "disconnect" between the client and their IT department. You might want to make sure that someone from the client's IT department is involved in the initial meetings/conversations so that they can understand what you are asking the client to do. If you are not comfortable with your level of technical knowledge you might want to take along support from a vendor so they can talk "Geek to Geek".

COLLECTION

Gathering ESI for further use in the e-discovery process (processing, review, etc.).

As a rough guide, there are two kinds of data collection, those that require a forensic process (complete with chain of evidence documentation), which is normally in cases of fraud, and the rest, where you just need to collect the data in a competent manner. The first group is a specialist area, and if you are involved in this kind of proceedings, you probably have got a "tame" forensic investigator that you can use, if not you need to find one. The forensic data capture might also involve things like retrieving data from mobile phones, making forensic copies of PC's or other computer equipment, and all other kinds of highly specific activities.

Turning to the more generic area of data collection, there are two schools of thought. One, is that you collect very broadly (so you only disturb the client once) and use the downstream processing to winnow out what you need. The other, is that you do a focused collection and run the risk of

having to come back and widen the scope. Each is valid, and they are none-exclusive, in that you can start focused and (if the case progresses/warrants it) come back later and do a wider collection for downstream culling.

This is where an understanding of the case, and where the information is stored is invaluable, as you can then make informed decisions. With, of course the price of the different options and how it affects the downstream processing very much to the forefront of your mind.

Forensic data collection organisations are a specific grouping of service providers. Make sure that you get a forensics company and not just a litigation support service provider that has sent someone on a data collection course. They tend to use products such as Guidance EnCase or Access Data's FTK toolkit to carry out the collection process, indeed this product is often used by the other group as well, just without the formalised chain of evidence documentation. The key thing is that people in this first group are used to appearing in court as an expert witness to explain how they obtained the specific piece of information.

The second type of data collection can be handled by a number of vendors, though in practice, using the specialist organisations and dispensing with the formal side of things is a sound tactic.

PROCESSING

Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.

The "shorthand" term for this stage is Early **Case** Assessment (ECA), or more accurately Early **Data** Assessment. This is where the range of options open to you increases quite dramatically. In the main the processing goes through two stages; first the data is "cleansed" in that unwanted types of information are automatically removed, this process can also involve the identification of duplicate versions of emails etc. Second, the data is loaded into a tool that allows the user to identify the information they want to take forward into the next stage.

The capabilities of the tools at this stage are quite bewildering, but in the main, you are trying to identify the information that you will want for your case, so an understanding of the key people involved in the matter (normally called data "Custodians" in techie speak) is good, as well as the date range that covers when key events happened. You might have an idea of the kinds of terms or key words that would be useful to search on, but there are other much more powerful technologies at your fingertips that will surpass the results of key words.

The key to getting maximum benefit from this stage is for you to team up with a sympathetic vendor and let them drive the technical process, whilst you supply the background and legal requirements of the matter.

The choice of software here is split into two groups. On the one hand there are products specifically designed to work in this area. These range from software that third party suppliers use, such as Clearwell, LAW or Nuix, through to tools specifically designed by suppliers for this area, like the ICE product from Palmer Legal Technologies or the snappily named MM/PC tool from eMag. There are a number of these specialist tools, and the mention of those above is not to elevate them above the rest, purely to show examples of the genre.

Secondly, there are emerging products from the next stages of the process (Review & Analysis), that incorporate functionality for this step as well. Products such as Lateral Data's Viewpoint come to mind as does the Access Data range, and Recommind's offerings. Again, these are mentioned as examples and not as an exclusive list.

Until recently the Early Data Assessment modules of the "All in One" products did not match the functionality provided by dedicated tools. This is no longer the case, which is good news in one way as it adds to the choices available to you, and bad news in another, as it adds complexity to the selection process in this area.

REVIEW

Evaluating ESI for relevance and privilege.

For many, this and the next stage form the hub of the eDisclosure process. The products mentioned here will be the environment in which you and your legal team will conduct most (if not all) of your on-line interaction with the data. The first half of the equation is the ability to review ESI and assign values for: Relevance, Privilege, Trade Secret, Personal Data, and as many case specific topics as you can shake a stick at. By the time you are in this stage, you should know what the issues are that you will be fighting the case on, and the various criteria you will apply to determine relevance et al. Your role will probably be to oversee the team that is carrying out this review work, though in smaller cases you might be doing the work yourself.

For large scale review exercises; you might have to recruit contract legal staff to do the work under supervision, you might have a "near shore" option of a cheaper office outside of London, you might be involved in an off-shore Legal Processing Operation such as Integreon (India), Exigent (South Africa) or Capita (Poland). In essence you will direct the team (whatever the size and geographical location) and provide overall Quality Assurance back to the Client.

In terms of who can help, the short answer is a lot of service providers. The broad split is between organisations that have their own software, and specialist software products that are supplied by different types of third party vendors be they consultancies (of different sizes) or more generic companies (that come from different backgrounds). There is a bewildering mix of software functionality and supplier personnel that combine to give you a multitude of options.

The key is that you should go through a procurement exercise before you are deep in the middle of a case, and thus make the decision in a rational cost effective manner, and not as a result of a frantic phone call to the first service provider you can find on a Friday afternoon.

ANALYSIS

Evaluating ESI for content & context, including key patterns, topics, people & discussion.

This stage is so interwoven with the previous one, that though they are separated for technical reasons, in practical terms they will often take place within the same piece of software (albeit in some cases with the assistance of specialist plug-in modules).

The trick here is to understand what you need to do, in order to meet the legal requirements of the case, and then how the technology can help you. By legal requirements I mean the issues of the matter as bounded by the court, cost and time. There is a scale of software tools available, and which ones you use are defined by the case, not by the product.

I find a useful analogy is the way in which it is possible to capture TV programs so they can be watched when we like. At the bottom end of the scale are VHS / Betamax video recorders, which are good for looking at something from start to end, but that's about it. So if you want to do a linear review in which you look at virtually every bit of ESI from "document" one to one million, then there are VHS litigation support equivalents that will let you do so.

If, however, you have a more complex viewing requirement and want the equivalent of Sky HD+ box that allows you to record three shows at once, pause live TV, access the past 7 days of

shows and download movies from on-line services, you want the litigation support products with more functionality.

There are lots of service providers who can help. The trick is to select one who can become a trusted partner, before it all starts getting too hectic.

PRODUCTION

Delivering ESI to others in appropriate forms and using appropriate delivery mechanisms.

You will want (have) to agree with the other side the scope of what you are delivering. The technical details of what is being handed over can mainly be left to the service providers, though you will probably need to give some guidance on how to handle "native" ESI, such as Word, Excel and PowerPoint.

Whoever is supporting your litigation software should take care of the technical aspects of exchanging information. You might need to work with them in understanding the implications of the options that the opposition give to you.

PRESENTATION

Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native and near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

This used to be a very US centric part of the model, however with the growth of systems such as Opus2's Magnum product, there is now functionality available in the UK. The key here is that you use these systems to start building the court room bundle well before the actual trial, all sides view the same documents (with access only to their own data on the ESI), and there are a variety of tools available to same time, effort and money.

SUMMARY

At the start of the process it is about you establishing the scope of the case, identifying the real issues, and then designing and driving the data collection and culling in an informed manner. You should NOT have to get involved in actual processing of data.

Once you are into the Review and Analysis stages, there is a very large range of options. The best advice is to carry out a procurement exercise, were you try as much as possible to compare Apples with Apples, for more advice on that side of things see the Buyer's Guide to Litigation Support Systems.

==========

Andrew Haslam, from Allvision Computing (www.allvision.co.uk), is the UK's leading independent litigation support consultant, who since 1997 has provided specialist legal IT advice and Electronic Data Disclosure (EDD) strategy to the UK's top law firms.

Andrew can be contacted on:

andrew.haslam@allvision.co.uk

+44 (0) 7789 435080

http://www.linkedin.com/in/andrewthaslam

@AndrewHaslam