LINEAL

TAMING THE BEAST:

ESI LOCATING AND COLLECTION CHALLENGES IN THE 2020S

What are the challenges litigation support teams will be facing in the 2020s?

In mid-2018, almost every single employee in almost every country in the world has the equivalent of a 1990s supercomputer in their pocket (or handbag). Think about that for a second. A mobile smartphone can now store as much critical information as an email server. In fact, sometimes more. From Facebook to Instagram, virtually every app a person uses is being used to collate data about them. And despite the bad press regarding how and for what purpose personal data is being harvested (think Cambridge Analytica), the horse has well and truly bolted on this issue. Despite the #DeleteFacebook movement, 2.19 billion people have a Facebook account, and Gmail boasts more than 1 billion users.

The effect of mobile on e-disclosure will revolutionise where discovery data is located and how it is collated. This presents an even greater task for law firms managing disclosure in civil litigation matters, especially given that many are still grappling to manage disclosure and costs around email.

Mobile data adds a whole new layer to e-disclosure mapping, preservation and collection, and this is likely to dominate the minds of Litigation Support Managers over the next few years.

A Litigation Support Manager at international firm, states that part of the problem litigation departments face when it comes to managing disclosure stems from failing to educate their clients on the Electronic Discovery Reference Model (EDRM) at the outset of their case, because:

a) They themselves are not up-to-date with the framework, and
b) The focus is usually on achieving an early settlement, meaning e-disclosure is left until the last minute.

"In practice, everyone leaves disclosure until a month before the disclosure report is due to be filed. Adding to this, clients will often say they only have a few gigs of data which needs to be combed through. This never turns out to be the case, once the data has been scoped properly, there is ***always*** a lot more to deal with".

Litigation Support Managers are currently dealing with two major challenges, namely:

- How to scope the data/documents which needs to be identified for discovery purposes, and
- Collecting the data/documents in a forensically defensible manner.

And often this needs to be completed within ridiculously tight timeframes and involve discovering and collecting data from multiple jurisdictions.

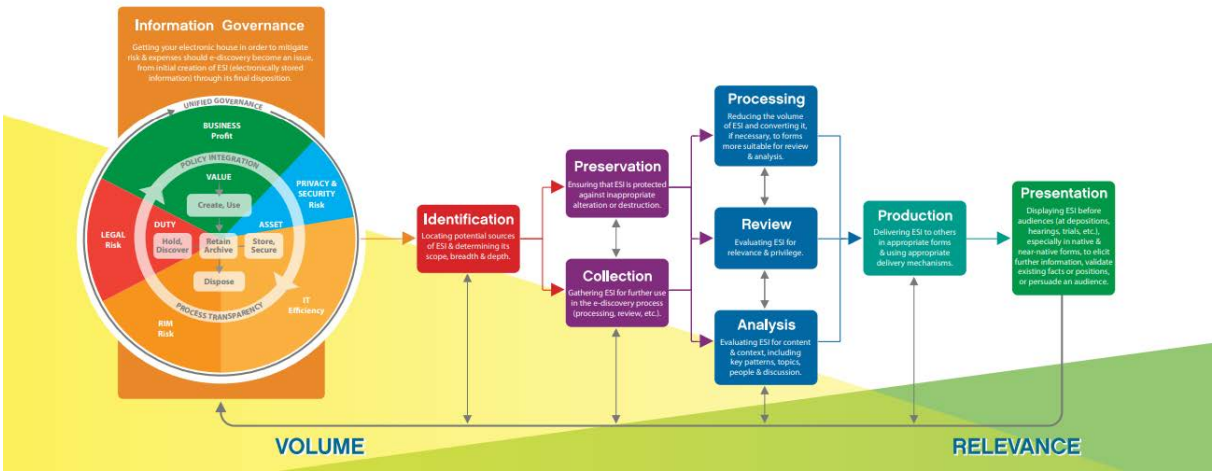
To be able to successfully meet e-disclosure requirements which are and will continue to grow exponentially with our ever-increasing reliance on mobile, not to mention, social media, litigators need to understand the following:

- The EDRM framework
- How to identify and locate Electronically Stored Information (ESI) that is potentially relevant to a particular matter quickly
- How to collect, organise, and preserve the ESI in a way that ensures it can be presented in court

The EDRM Framework

Created by George Socha and Tom Gelbmann, to address the lack of standards in the e-disclosure market, the EDRM framework is the starting point for any discussion on e-disclosure. Comprised of nine different stages, it acts as a map for project teams staring down the vast gulf of possible ESI which may need to be located, preserved, collected, and reviewed.

What follows is a brief guide to the nine stages:



Information Governance – refers to a set of structures, policies and procedures, and controls which exist to manage an organisation's information.

Identification – this involves established which ESI is relevant so that it can be preserved for disclosure purposes.

Preservation – protecting ESI from being deleted or spoiled is usually achieved by placing a litigation hold (or legal hold as it is sometimes known), over them.

Collection – relevant data and documents must be collated and centralised, in a ***legally defensible way*** (more on this later).

Processing – here the ESI is prepared for review. This is typically done using specialist software.

Review – the ESI is analysed and checked, not only for relevancy, but for litigation and legal professional privilege. This process, the most expensive part of e-disclosure, is becoming increasingly automated.

Analysis – despite being placed under review, the analysis of the documents occurs at many stages of the process. At its peak, analysis involves examining the ESI for patterns, topics, people and conversations.

Production – producing the ESI to be used as evidence.

Presentation – how the disclosure ESI is presented as evidence in court.

Although the EDRM framework has been updated, it is 13 years old. When it was developed, social media was in its infancy, and the most sophisticated messaging system was text. In addition, the software available to perform e-disclosure tasks has moved on light-years from that available in 2005.

And then there is the continued problem that the framework was designed for e-disclosure around ***documents***; as we have established, the biggest challenge moving forward into the 2020s relates to ***data***.

Identifying and locating potentially relevant ESI in a timely way

The key to success in e-disclosure is to begin the process as soon as an instruction is received. Start by assembling a project team, ideally comprising of in-house Counsel, someone from the IT team, someone from the records management team, a senior representative of outside Counsel, and an external E-Disclosure Consultant.

Another element of the e-disclosure process (often neglected) is to document ***every*** action taken by the project team. Doing so will ensure you can defend the position you have taken.

In *West African Gas Pipeline Company Ltd v Willbros Global Holdings Inc* [2012] EWHC 396 (TCC) the Technology and Construction Court (TCC) made a wasted costs order against a party where there had been "serious mistakes resulting from an inadequate initial review and gathering together of a complete set of electronic documentation".

Mr Justice Ramsey stated:

> "*Disclosure in complex international construction projects is always difficult but there is no doubt that WAPCo's disclosure in this litigation has caused a number of additional problems. Those problems, particularly in the context of electronic disclosure, mean that time and costs have been wasted as a result of errors made in providing WAPCo's disclosure. I accept that there must be some give and take between parties and their solicitors in relation to difficulties which inevitably arise in the course of e-disclosure and require to be dealt with by cooperation by the parties and their lawyers. However, there will be cases where the court may properly exercise its discretion and make an order for one party to pay costs under CPR44.3 if, having regard to all the circumstances, the conduct of a party in relation to disclosure justifies that order. It is, in my judgment, only generally in cases where there had been a mistake or error which has had significant consequences in terms of time and cost that the court will generally make an order for costs which have been wasted".*

The first step to identifying and locating ESI for e-disclosure purposes is for the project team to discuss with the client how they store and manage electronic information. Most Litigation Support Managers believe such discussions are always best done face to face, as few clients truly understand the nature and extent of the ESI which may be subject to disclosure.

Even if there is the strong possibility of an early settlement, it is never too early to start the identification process. Not only will good organisation allow you to comply with your disclosure obligations, project teams need time to recognise any potential issues which may arise in the disclosure process, for example, a client who is reluctant to divulge certain information, the existence of personal mobile devices which may hold key material, and/or the existence of a server located offshore. In addition, an early start on the disclosure process can assist you with preparing a more accurate cost assessment for your client and/or as required under CPR 3.12, and to propose a realistic, sensible, and proportionate disclosure order.

Project teams should anticipate that the disclosure project is likely to change as the matter progresses. However, having a detailed data map, not only of the data held by your client, but also any third parties, will put you in a strong position to respond quickly when such changes occur.

It is at this stage you may want to consider instructing an e-disclosure consultant. Although the court does not require the project team to have specific technical qualifications, you are expected, as a firm, to seek appropriate advice as required. Although there is a cost attached to bringing on an e-disclosure expert, this needs to be balanced against the costs which can be saved with an efficient and effective e-disclosure process. Not forgetting that there is a risk of cost sanctions being applied if the disclosure process is not properly managed.

In her article, *Avoiding errors & pitfalls in eDiscovery*[1], Julia Chain advises:

> "*During collection, the lack of a developed and detailed data map can leave the parties exposed to potential issues as a project moves through the 'electronic discovery reference model' (EDRM). In high risk, high-speed matters with strict deadlines, if the location of key data is not properly identified, disruption and delays can easily occur during the course of a disclosure exercise. A robust information governance protocol, including any number of general best practices related to organising data, can help create an environment where electronically stored information is easily identified, as well as accessed and collected. From a data protection perspective, an effective information governance protocol also helps an organisation comply with the many data protection obligations imposed on corporations*."

Collecting documents in a forensically defensible manner

Once the ESI has been identified, the next step is to ensure it is collected in a way that does not compromise its ability to be used in court. A sure-fire way of risking the forensic credibility of a document is to copy and paste it from one file to another, thereby modifying the date.

The best way to preserve the metadata and structure of a document is to employ specialist e-disclosure software at the collection stage. There are several suppliers in the market; therefore, it is good practice to establish relationships with a number of service providers, perhaps keeping a preferred supplier list. Some firms prefer boutique vendors who they can build a long-term relationship with, one Litigation Support Manager comments; "*Our guys are dependable – we know they will get things done. They also understand the quality of the work that needs to be turned around and they are familiar with our firm's expectations*".

[1] N.L.J. 2017, 167(7764), 20.

When collecting ESI, it is important to:

- Consider any obligations under the General Data Protection Regulation (the GDPR). The GDPR introduces substantial amendments to EU and UK data protection law and makes provisions in relation to the processing of personal data and the free movement of such data. Typically, evidence involved in the disclosure process will include personal data. Clients and legal advisors may be data controllers and/or data processors and as such will need to comply with the GDPR. The processing of personal data is permitted under the GDPR where there is a legitimate basis laid down by law, such as a court order for disclosure, but issues may arise, for example, in relation to the processing of personal data that is not clearly within the scope of a disclosure exercise.
- Question what is reasonable and proportionate when considering how much and what form of data to capture.
- Confer with other parties and their advisors on the methods used to collect the data and the overall scope of the collection.
- Ensure that any decisions not to search for a category or class of document are justifiable, i.e. because to do so would be ***unreasonable***. This is where documenting the project team's processes and decisions comes into play.
- It is good practice to set a budget for disclosure costs and regularly review it.
- Make sure the central storage location is large enough and has the appropriate security in place, especially if the legal matter is a highly sensitive one.
- If documents are held in offices or off-site storage in another country you need to check you are not breaking any jurisdictional laws by collecting them. To do this consider whether you need to obtain legal advice from local law firms.

Ideally, collecting ESI should be done by an independent vendor who has both the understanding of the complex nature of collecting the material in a forensically defensible way and has the tools available to achieve this objective.

Identifying and collecting mobile data

Mobile e-disclosure bears little relation to the traditional document-based e-disclosure model. Therefore, it is important for litigation support teams to start thinking of the two as separate forms of e-disclosure and adapt their review processes to fit the requirements of each one.

As one US attorney put it:

"Mobiles different, it does not answer our questions in quite the same way. It requires new eyes to be able to discern what it is we get out of mobile….we have to adapt the questions to the data rather than the traditional approach – a linear review of communications such as email".

E-disclosure vendors in the UK have successfully been identifying and collecting data from devices such as smartphones, iPads, drones etc. for several years. If information is held on a personal device which is also used for business purposes (i.e. to access company emails), the personal data can be filtered using keyword searches etc.

Complications can arise if data relevant to disclosure is contained on an employee's personal device and they are reluctant to hand the device over to the project team. In such an event, a court order can be sought to force the employee to comply.

When it comes to personal data, the General Data Protection Regulations (GDPR), which came into force in May 2018, now require project teams to be even more mindful of separating personal data which is not relevant to the proceedings and make sure it is redacted before it is disclosed. The GDPR also has the potential to increase costs for a law firm in circumstances where a person wishes to have access to personal data collected for the purposes of disclosure. In most cases, the data owner does not have to pay a fee to access the data an organisation has relating to them, which can result in a law firm having to undertake a costly data retrieval exercise. Working with a vendor who has access to tools which can quickly filter out irrelevant personal data mitigates the risk of having to undertake such an expensive process.

Mobile e-disclosure requires different methods to be employed by the project team, as unlike a computer or server, the device cannot simply be opened up and forensically imaged or copied in pieces. As well as separating business and personal data, other issues must be considered, such as mobile data stored in the cloud, the devices operating system, encryption, and mobile device management software.

Adding to these challenges is the fact that most mobile phones are now subsidised by the network provider, who offer an upgrade every two to three years. Furthermore, devices are constantly being updated during their lifecycle. Forensic software is therefore always playing catch-up with the latest developments by providers, therefore, going forward, it is likely only specialist e-disclosure vendors will have the technology and expertise required to identify, locate, and collect mobile data successfully.

Concluding comments

Those of us who remember the days before ESI may think the world has changed at an unfathomable speed and maybe e-disclosure methods are beginning to catch-up, albeit, slowly. We can now extract ESI from drones; how will we extract information and data contained in a company-owned self-driving car? Or the knowledge contained in a robot which has intelligence which exceeds that of a human. These questions may sound like they have been drawn from a sci-fi movie, but the fact is the AI revolution will transform everything about our world (including our legal system) far faster than the digital-age has done. Investors are confident enough to put money behind this prediction, with an estimated $15.2 billion of venture capital going to AI startups in 2017 and Alphabet/Google acquired Deepmind, a 700-strong team focused on AI research in 2014.

Given the huge push occurring in the AI sector, the challenges relating to ESI identification, location, and collection in the 2020s and beyond could well be focused more on retrieval from AI as well as mobile. And litigation support teams may look upon the e-disclosure challenges associated with email with fond memories, referring to this period as “the good old days”.

Lineal has extensive experience in all aspects of eDiscovery. To find out more about predictive coding, eDisclosure and our other services, please call us on +44 (0)20 7940 4799 or email info@linealservices.com.

Lineal Limited
125 Finsbury Pavement, London, EC2A 1NQ
+44 (0)20 7940 4799
www.linealservices.com