REPRINT

CD corporate disputes

UNDERSTANDING E-DISCLOSURE – MANAGING PEOPLE, INFORMATION AND DEVICES

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
OCT-DEC 2018 ISSUE

www.corporatedisputesmagazine.com

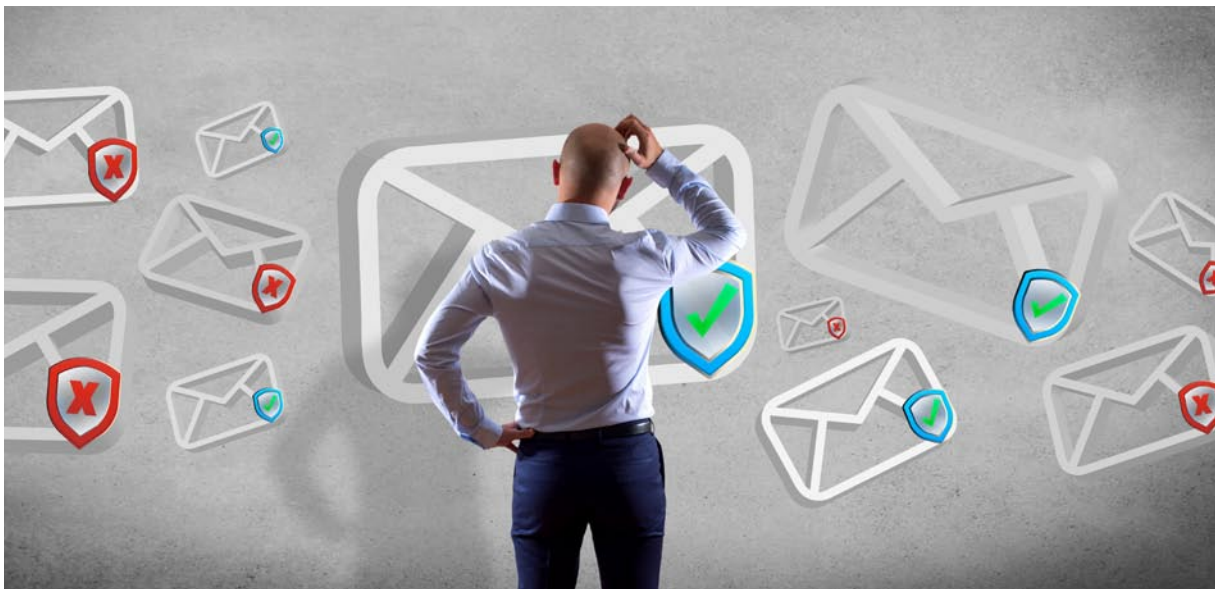
Visit the website to request
a free copy of the full e-magazine

itgroup
Clarity in Technology Disputes

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

MINI-ROUNDTABLE

UNDERSTANDING E-DISCLOSURE – MANAGING PEOPLE, INFORMATION AND DEVICES



PANEL EXPERTS

George Jennings
Head of Digital Forensics & e-Disclosure
IT Group UK
T: +44 (0)845 226 0331
E: george.jennings@itgroup-uk.com

George Jennings is head of the digital forensics and e-disclosure department at IT Group. He is responsible for the continuous development and expansion of the firm's e-disclosure practice. He is an expert in the field of forensic technology and has been instructed by many of the leading law firms in the UK and overseas.

Jake Ridley
e-Disclosure Supervisor
IT Group UK
T: +44 (0)845 226 0331
E: jake.ridley@itgroup-uk.com

Jake Ridley is responsible for the day-to-day management of the e-disclosure department at IT Group. He plays a predominant role in the project management of all matters handled by the e-disclosure team and provides ongoing support to parties during every stage of the e-disclosure lifecycle. He has been involved in a number of large-scale digital and regulatory investigations, working for leading law firms in the UK and overseas.

Kieran Maher
Systems & Software Consultant
IT Group UK
T: +44 (0)845 226 0331
E: kieran.maher@itgroup-uk.com

Kieran Maher is a software and systems consultant at IT Group. He is an active programmer, specialising in web-based technologies, and also acts as an in-house developer when the need arises. He is a specialist in technical systems and software, with particular commercial experience with web technologies and development, and software-based development with respect to commercial litigation.

CD: In broad terms, could you explain why well-defined data management systems are important for e-disclosure in the context of a dispute?

Jennings: The fundamental principle of a data management system is to enable authorised, reliable and secure access to, and storage of, electronically stored information (ESI). In the context of e-disclosure and the duties associated with the disclosure exercise in law, the key elements are to be able to demonstrate that a thorough search has been carried out and relevant data has been harvested, all within the context of proportionality. The more comprehensive the data management system is, the easier it is to harvest an appropriate data subset, thus saving costs and time associated with presenting and reviewing large data sets. In summary, maintaining a well-managed ESI estate, which includes robust archiving abilities, is imperative should a disclosure exercise be required.

> **"The fundamental principle of a data management system is to enable authorised, reliable and secure access to, and storage of, electronically stored information (ESI)."**
>
> *George Jennings, IT Group UK*

CD: What specific obligations does the e-disclosure process tend to entail for parties involved in a dispute?

Ridley: The identification, preservation, collection and production of potentially relevant evidence is the predominant obligation for parties involved in a dispute. It is the duty of the parties' legal representatives to explain to their clients the importance of preserving potentially relevant, and therefore disclosable, documents in addition to the requirements necessary to make the documents available in an agreeable format thereafter. In order to conduct the process successfully, it is vital that parties agree the parameters of the e-disclosure process early on in proceedings. Taking the time to agree an execution plan early on may avoid the potential for disputes relating to the way in which the disclosure was conducted emerging later down the line. In English law, the parties should consider using the electronic disclosure questionnaire (EDQ) at the outset to guide the identification and management of their client's and also that of their counterparty.

CD: What steps should parties take to effectively manage people, information and communication devices for e-disclosure purposes?

Maher: Organisations should implement robust and comprehensive information governance and data processing policies, not only in anticipation of e-disclosure, but also to ensure effective information management generally. Taking steps to reduce the volume of unnecessary data organisations store will make it easier to identify and access potentially relevant data for e-disclosure purposes when the need arises. Implementing an effective and well-managed information governance strategy will enable parties to make a well-educated assessment of what systems they have, what material they hold and what data, if any, is controlled by third parties. Preparing and maintaining an up-to-date register of key data repositories and devices, and who within the organisation has access to them, is advisable. This could prove critical when establishing key custodians and communication devices during the e-disclosure process.

CD: In your experience, what are some of the common pitfalls of e-disclosure which can be mitigated or overcome with effective planning?

Jennings: If parties do not seek appropriate external expertise and guidance, issues may arise due to the mismanagement of the identification and processing stages of the e-disclose process. Incorrectly identifying key data sources, custodians, date ranges and other vital criteria can lead to the aggregation of irrelevant documents which could be an added expense to process. Effectively culling irrelevant documents is critical as this will save vital time during the review process, which many parties often observe to be one of the most costly stages of e-disclosure. In a similar vein, failing to

> **"The identification, preservation, collection and production of potentially relevant evidence is the predominant obligation for parties involved in a dispute."**
>
> *Jake Ridley, IT Group UK*

optimise documents for review is also a common pitfall. Organisations that deal with large quantities of physical documentation that requires scanning need to run the electronic copies of their documents through a process called optical character recognition (OCR) in order for the documents to become searchable and responsive to keyword searches – a critical element of the e-disclosure review process. Engaging with an e-disclosure specialist from the outset will mitigate these challenges.

Maher: A common objective of e-disclosure is to replicate the file structure of the target system as closely as possible. If the system being replicated is unstructured and overly complex, recreating an effective structure will be much more time-consuming. Parties must also consider the impact on document metadata, which describes elements of information such as 'last modified', 'date created' and 'last accessed' during the identification and collection stages of e-disclosure. A common pitfall occurs when the metadata is not preserved. It is critical that parties take particular care to ensure that the integrity of the data is maintained prior to and during the collection process to prevent any inadvertent or deliberate alteration or deletion of critical documents. Failing to adequately preserve data can lead to complications during the review process. For example, if the metadata is modified during the collection process, it can impact the legitimacy of the document and also the document's responsiveness to search criteria. Imagine a scenario where you have claimed to have a documented policy in place since 2008, when the 'date created' on the document you disclose suggests that it was created last week because the metadata has been inadvertently updated. These are the scenarios parties want to avoid as they may face criticism from the other side. Parties facing litigation should seek guidance from an e-disclosure specialist with forensic collection capabilities who can not only assist with identifying and scoping potential data sources, but can collect the data in a forensically sound manner, ensuring that all metadata is preserved.

> **"If the metadata is modified during the collection process, it can impact the legitimacy of the document and also the document's responsiveness to search criteria."**
>
> *Kieran Maher, IT Group UK*

CD: In your opinion, how important is it for companies to train key staff in e-disclosure techniques? What benefits might this yield if a dispute escalates to litigation?

Ridley: The last place an organisation wants to find itself when facing litigation is on the back foot. Ensuring that key personnel are well educated on the processes that govern e-disclosure is critical. In doing so, you communicate to the courts and to your counterparty, that you have a well structured and methodised strategy for e-disclosure in place. Also, ensuring that employees are up to speed with the latest search technologies, as well as techniques for conducting the review process, is paramount. During the review process, the ability to effectively analyse the content of a document for relevance is key. Legal teams need to be confident in their ability to establish the context of a document quickly by successfully identifying key themes, topics and discussions.

CD: With e-disclosure often expensive and time-consuming, what can companies do to keep costs in check and store data so that it is easily accessible now and in the future?

Jennings: A lack of understanding about how much data there is to consider and where it is stored is often what leads to spiralling costs during e-disclosure. Many e-disclosure platforms charge for processing per gigabyte, so understanding how data volumes might be reduced before processing could lead to direct cost savings. Further, instilling a workplace culture that is mindful of document handling, efficient document versioning and appropriate storage, retention and purging practices will significantly ease the time burden associated with identifying relevant data sources. It is also critical that parties identify the parameters and scope of the e-disclosure exercise at hand from the very beginning and continually audit progress throughout to keep costs in check. Agreeing keywords, date ranges, custodians and the process for exchange early on will ensure that the e-disclosure exercise is planned and managed properly, and conducted in a timely and cost-effective manner.

CD: What essential advice would you offer to companies in terms of establishing effective e-disclosure policies and procedures which provide oversight of all pertinent obligations?

Ridley: E-disclosure investigations can be drawn out and complex. Putting efficient and appropriate procedures in place is essential to get the right results and reduce time and associated costs. We would also advise parties to seek and instruct an e-disclosure technology provider that offers complementary consultancy and project management services that can take the strain out of the process and help avoid the potential pitfalls. Ideally, parties need to seek a single end-to-end service provider that can assist at every stage of the e-disclosure process, from data collection to exchange and management and maintenance of the review platform. When seeking a provider, it is important to consider other additional costs, including document OCR, password cracking, email threading and production bundle creation, as these costs will often be unexpected and unplanned for at the outset.

CD: How do you expect e-disclosure to evolve in the years ahead? What key trends do you expect to impact the process?

Maher: The number of files that users are storing in encrypted formats will continue to rise as more emphasis is put on keeping confidential or privileged data secure. Encrypted files are not problematic if the passwords are known, but otherwise can be time-consuming to deal with. Increased levels of encryption on smartphones will ultimately play a part in data extractions. The use of cloud-based storage will continue to accelerate which, in itself, is not problematic but does lead to differences in the metadata and often impacts the ability to recover deleted material. Other storage devices, such as Internet of Things (IoT) devices, may be in scope for searching for relevant material, which will lead to more specialised harvesting techniques needing to be employed. Furthermore, as confidence grows in machine learning and predictive coding, the need for junior legal teams to conduct the 'first pass' phase of removing irrelevant documents will reduce. CD