

LITIGATION SUPPORT

UK firms would do well to follow the lead of their US compatriots in embracing electronic disclosure, or else risk falling behind in the competitive legal services market, says **Kelvin McGregor-Alcorn**

Playing catch up

UK law firms need to follow the example of their US counterparts and embrace electronic discovery if they are to remain competitive in the increasingly global legal services market. Electronic information is the new frontier and litigators have to venture into it whether they want to or not.

In an era where over 93% of all documents are produced electronically, with over 75% of those never making it to the printer, 'smoking gun' evidence is more likely to be found lurking on a computer than buried in a filing cabinet. The most effective way to search for this key information is electronically.

Lawyers in the main still think in terms of reviewing paper and in the UK still have little practical appreciation and experience of the benefits of using technology to support their discovery. They are also facing a further challenge of operating in a legal environment where case law is still evolving.

Discovery of electronic data cannot be ignored. It is something every lawyer will have to come to terms with, whether in local government, a high street practice, an international corporation, or a major international law firm.

In the US, the disclosure of electronic documents has already become standard procedure. Since it is easiest to learn from the oversights of others, what follows are some of the most common mistakes US litigators have made while navigating the electronic disclosure frontier.

Having no electronic disclosure plan or pursuing electronic disclosure in a haphazard manner

A litigator is unlikely to find a key document in a box located in a remote storage facility. Litigators who take the time to learn what e-evidence is, how to find it, how to use it and how to avoid problems when dealing with it increase their chances of prevailing in a case and avoiding judicial sanction. Today in the US, almost every case strategy includes an electronic disclosure component.

Not understanding that delete does not really mean delete

Far too many educated and sophisticated business professionals have learned this lesson the hard way. US case law is full of civil and criminal decisions where the individual did not understand that the 'delete' key on the keyboard is not the equivalent of the paper shredder.

Each and every electronic document leaves an electronic fingerprint. This fingerprint is then stored or captured on the hard drive, even if all that you do is open a document from a floppy drive and send it to the printer. The fingerprint remains magnetically

embedded on the drive (and ripe for the picking by computer forensic experts), regardless of the fact that you direct the computer to delete the data. Only until you resave over the fingerprint, which typically occurs when the all hard drive space has been utilised, might the fingerprint disappear for good.

Underestimating e-mail use

Employees create more electronic evidence than you think. Many parties have found themselves in the middle of a minefield for not producing electronic evidence from custodians that seemingly 'did not use their computers much'. Keep in mind, if the court issues an order directing retrieval, or, worse yet, the opposing party happens to have e-mail from that individual and those records were not produced, it could give the appearance of impropriety and may lead to sanctions.

Failure to image hard drives of departing employees

It is important to have a policy in place for handling the electronic business records of all departing employees. Often, a simple bit-by-bit copy of the hard drive (known as a mirror image) may be extremely useful in the event litigation ensues. There is nothing more frustrating to a litigator than to be in the midst of disclosure and hear 'that information is on John's laptop and we let him take that out-of-date machine with him when he left'.

No back-up or document retention policy

A company's failure to have a document retention policy may raise red flags. The bulk of the retention policy should include a method for determining retention periods, the retention schedule, the retention procedures and a records custodian.

Failure to fully discontinue document destruction practices

A corporation cannot blindly destroy documents and expect protection from a document retention policy. In the wake of a pending or impending suit, your clients must immediately halt all electronic document-handling policies that result in intentional or negligent destruction of potentially relevant evidence.

It is critical to reach the individuals that actually carry out the document destruction to ensure that preservation is properly and completely enacted.

Ignoring certain 'hard to deal with' sources of evidence

It is easy to ignore 'hard to deal with' media types, such as out-of-date back-up tapes or hot off the market personal digital assistants or electronic tablets. However, many times these media sources are where the smoking gun documents are located.

No longer is it appropriate to hide behind the

technology, claiming that the systems are too antiquated, damaged, or burdensome to be searched for relevant documents and e-mail. There are a vast number of experts that are well-equipped and professionally trained to assist in this task. With this type of challenge it is important to get them involved early.

Claiming to have produced everything or turning over electronic data late in the day

In the US it has been held that where a party breaches a discovery obligation by failing to produce e-evidence or excessively delaying the production of e-evidence, the court has broad discretion in fashioning an appropriate sanction. Such sanctions can include delaying the start of a trial, declaring a mistrial, issuing an adverse inference instruction, or ordering monetary penalties. They may be imposed where a party has not only acted in bad faith or grossly negligent, but also through ordinary negligence.

Inexperienced people conducting well-intentioned forensic investigations

When an incident occurs there is a strong tendency to have the security or technical staff 'take a quick look' at the suspect's computer in an attempt to confirm or deny suspicions. Unfortunately, the act of taking a quick look, if not carried out using proper computer forensic protocols, often results in unintended and unnoticed changes to the digital files. For example, simply booting up a computer can destroy temporary files and change file dates/times.

Seeing electronic discovery as an exclusive 'in-house' responsibility

Some companies have chosen to handle electronic discovery requests in-house on a case-by-case basis. However, as one author recently noted: "It is unrealistic to assume that IT professionals can pay attention to all the nuances of litigation, manage the lifecycle responsibilities associated with e-mail, and enforce an overall e-mail archive policy. Companies will be caught off guard by assuming that IT can shoulder this burden alone."

Depending on the complexity of the technology involved, intricacy of the request, judicial deadlines, exposure to liability and diversion of internal staff, you might want to consider consulting an electronic evidence expert to help manoeuvre around any potential stumbling blocks.

No longer can parties or their counsel claim to be unaware of the new frontier of e-disclosure. Keeping abreast of the changes in technology and the law will help UK litigators avoid similar mishaps and become more effective in the digital age.

Kelvin McGregor-Alcorn is a director at Kroll Ontrack.