HILL DICKINSON

Morphed in the medium, the Needle in the Haystack and the Perils of E Disclosure

Electronic communications and systems have increased the speed of transfer of thoughts and hugely increased the number of messages; we are each bombarded with information. These systems have irrevocably changed the way that business and litigation is conducted and created new risks.

Morphed in the medium

In the past, the physical difficulty of writing and later typing regulated in some measure what was created and what was sent. Letters were shorter and crucially there was more time to think. Post and contracts could be signed, say, only by managers or directors and communications would be filtered through the sensibilities of secretaries.

The advent of the word processor, but most particularly of email, then text messages, messaging systems, and, in some businesses, social and business networking sites, has changed the landscape beyond recognition. All grades of personnel can now easily create messages, by email and possibly by text and instant message, and send them out. Supervision may be difficult or impossible, minimal or non existent. And remote working makes the risk more acute, as the PVM Oil Futures allegedly drunken oil trader case (BBC News on line 29th June 2010) so eloquently demonstrates.

Further, the ease of creating and sending has been coupled with a significant change in business etiquette; the language has morphed in the medium. Many who generate messages and records cannot type; so text is foreshortened. The customary salutations and courtesies of correspondence have been eroded. It is increasingly rare in email, and certainly in text and instant messaging systems, to express thanks or to ask permission. The choice of vocabulary has changed, often shorter, blunter. And moreover the boundaries of what is acceptable (or what people *think* is acceptable) in the work environment have been eroded. The informality of the medium has encouraged informality and indiscretion in content. Thus:

"It is well known that people say things in e-mails which they would not dream of putting into a letter or a minute or a formal note..." (*Digicel (St Lucia) Ltd v Cable & Wireless PLC* [2008] EWHC 2522)

And with the bombardment of incoming messages there is a parallel, irresistible desire to reply immediately, with the lurking danger of the "reply to all" button. Just because the message has been delivered quickly there is an unreasonable expectation that a fast response must be provided; in the mind of the sender and the receiver. But act in haste, repent at leisure. Emails, for example, can be distributed by the creator or recipient, intentionally or unintentionally, to a vast audience at the touch of a button, with devastating consequences, including, the loss of legal advice privilege or the onward publication of a libel.

Other hazards are obvious; the risk of misunderstanding and easy offence which may disrupt otherwise smooth business relationships and the creation of records which are inappropriate for the business environment and potentially compromising to the defence or prosecution of claims.

These new electronic systems have, therefore, created new risks for business and for individuals. There is a pressing need to regulate how individuals within business express themselves, in the documents they create, in the messages they send and in the records they keep as part of routine daily work. And the more business relies on remote communication in a text format, on computer and other electronic communications systems generally, rather than discussion face to face or on formal correspondence, the more pressing the problem.

The Needle in the Haystack and the Perils of E-Disclosure

Litigation and arbitration fall into certain basic phases; Pleadings, where the parties make their allegations and set out their case, Disclosure, where each side produces to the other for review all documents relevant to the matters in issue (with the important exception of privileged documents like legal advice), exchange of Witness Statements, exchange of Experts Reports and Trial/Final Hearing.

Disclosure is regulated by Part 31 of the Civil Procedure Rules. Particular rules are under development for E Disclosure. This is an evolving field. A review of Part 31 is beyond the scope of this note, but the scale of the task it imposes can present a significant challenge in the management of any case.

Disclosure is a key phase; a first glance at part of the evidence to assess the allegations in the pleadings. Once it was a relatively straightforward matter confined to hard copy documents; letters, memos, reports, accounts, slips, wordings, policies and the like. These new electronic systems have, however, irrevocably changed the conduct of legal process, whether arbitration or litigation. Disclosure means that parties will have at some stage to produce electronic records for review by their opponents. The process may be costly because there may be huge quantities of data. And there is the increased risk that such "documents" may be damaging to the prospects of defending or prosecuting claims; or at the very least embarrassing and damaging to business relationships. Electronic disclosure is now a matter of routine, but whether it is done well is quite another matter.

There are two particular problems we touch on here; first that the necessary disclosure may not be found and produced for inspection and… secondly, that it will.

It will not be found

A whole industry of experts has grown to manage the efficient gathering collating and analysing of such electronic data, with ever more sophisticated software search systems. There are hazards here for the unwary. In Earles [2009] EWHC 2500 the judge found that neither party had given proper disclosure and consequently neither had taken steps to preserve potentially relevant phone or email records. The court found that the conduct of e-disclosure by the defendant bank had fallen below expected standards and took this into account when allocating costs; a serious consequence.

The trial judge, commenting on the 'Earles' case in a seminar speech earlier this year (March 2010) observed that it:

".. exposes serious flaws in the understanding and practices... even in blue chip firms and companies, of what is required in electronic disclosure and the lack of

data control, retention and readiness strategies in even the largest most sophisticated organizations where electronic records are a modern way of business life".

It will be found

Conversely, those responsible for data creation and management should assume that if an "unfortunate" document or message has been created it *will*, like the needle in the haystack, be found.

All of these new systems create "documents" and store them on PCs, central servers, back up servers Blackberrys and mobile/cell phones. An indelible digital footprint is created; it does not disappear but lies waiting. What may then come as an uncomfortable surprise to potential litigants (and their employees) is the range and depth of the probing that E-Disclosure may entail. It can require the production of all relevant records from central servers, personal computers, laptops, back up tapes, mobile telephones, notebooks and the ever growing list of hand held devices. This can include mail, calendar, spreadsheet and document files. All the so-called meta-data may also be recovered (original author, creation date, hidden notes, amendments, identity of blind copy parties). And deletion may not be a wise way to attempt to remove inconvenient material; even after deletion it may be recovered from hard disks (as demonstrated most recently by the Chelsea barracks litigation, BBC News on line 25th June 2010).

And with the practice of copying messages and reports ever more widely to large numbers of recipients the likelihood of being pricked by the needle in the haystack is that much greater.

Conclusions

The management of any form of written communication or record keeping is a key element of risk management, as is remote access to business systems. It is likewise a key aspect of the management of cost in actual or potential litigation. And there may be insurance coverage issues.

E protocols, what you could or should send and receive, what you could or should create, are obviously essential, but if these are primarily a device to regulate behaviour *after* the event (work place discipline) they have largely missed the point. Giving lengthy protocols to employees, managers and directors can often be a complete waste of time. They may never be read (even if they are *"signed as read and understood"*).

The hazards of e-commerce need to be explained in person, with examples of the alarming pitfalls so that the problem is genuinely understood such that a moment's inadvertence should not lead to a lifetime of regret (we are running talks on the subject).

Businesses need to give careful thought to what is required in electronic disclosure and to *"data control, retention and readiness strategies"*. It may be too late if such thought is only applied after a dispute has arisen or proceedings have been commenced.

Note: this is an updated and amended version of an article first published by the Chartered Insurance Institute, the original of which can be found at http://www.cii.co.uk/knowledge/londonmarket/.