

“Caught In Conversation”

Electronic Communication – The Pitfalls

You're in the office. It's late, and you want to go home. But you have a disclosure deadline fast approaching on your current case. You decide to review one more file of documents. Less to do tomorrow, you think, and it'll be a quick job. And then . . . you come across the innocent but fatal e-mail . . . your heart sinks . . . what was that robust line of defence you had been discussing with your client only yesterday . . . I think we need to discuss settlement, you tell your client the next day. But, I don't understand, says the client. An e-mail is not a document. It's just a form of conversation, electronic conversation, like the texts I send and the messages from my BlackBerry . . .



On 1 October 2005, provisions dealing specifically with the disclosure of electronic documents during litigation came into force. Practice Direction 31 to the Civil Procedure Rules (CPR), which deals with the disclosure and inspection of documents, now includes a section on electronic disclosure (see Para 2A), and there is a new form of Disclosure Statement which contains detailed references to electronic document searches (see Annex to Practice Direction).

The law

For disclosure purposes, the word ‘document’ has always been defined broadly as being anything in which information of any description is recorded (CPR 31.4), i.e. including electronic documents. But the new electronic disclosure provision spells this out and makes it clear that the definition of document in CPR 31.4:

“. . . extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been ‘deleted’. It also extends to additional information stored and associated with electronic documents known as metadata.” (PD 31, Para 2A.1)

And the person signing the Disclosure Statement now has to specify the electronic searches he has made by reference to a list of electronic media (which include mobile phones and handheld devices) as well as electronic applications (which include web based applications).

Is business keeping up?

So, technology continues to develop at breathtaking speed, and the Courts are clearly keeping pace. But what about the world of business? How is it keeping up with developments in the litigation world?

We spoke to three people who have to address electronic document risk on a daily basis: Joshua Bayliss, Group General Counsel for Virgin Management Limited; Alistair Wyvill, a barrister at St Philips Chambers in Birmingham; and Mark Carver, Vice President – Professional Liability at AIG Europe (UK) Limited.

“...In one recent case, a witness had forgotten about the data trail stored on his computer... which didn't quite accord with his recollection of events.”

**Joshua Bayliss, Group General Counsel,
Virgin Management Limited**

For Joshua Bayliss, electronic communication is a fact of life. That's how business is done today. Most correspondence is by e-mail (he typically receives more than 100 e-mails each day), and at meetings many of those attending will be taking notes on their laptops or BlackBerries as they go.

But while electronic communication speeds up business, it can be a real headache for in-house counsel. When it comes to litigation, a business will need to disclose relevant documents, including any electronic communications. But has it kept a record of these? And what about employees? Were they aware at the time that their e-mails might have to be disclosed in the future?

The reality, says Joshua, is that people need reminding that e-mails are documents. People often tap out e-mails without thinking that they might be creating a document, because e-mail is much closer to a form of conversation. And they put things in an e-mail which they



wouldn't write in a letter. The problem is even worse with BlackBerries. Against this background it is important to have good document management and retention policies in place, and to provide effective training in order to maximise the prospect of their being followed. In addition, a business needs to have a protocol for exiting staff which ensures that

all information on their computers (particularly laptops) is captured before they leave. There are companies which have found themselves in the difficult position of having to decide whether to initiate proceedings against a former employee to recover information.

"...And they put things in an e-mail which they wouldn't write in a letter. The problem is even worse with BlackBerries."

Data retrieval is also becoming an increasingly important issue. With companies opting to store records electronically for reasons of space and cost and computer systems constantly changing, Joshua points out that a business will need to make sure that it retains all the hardware necessary to access superseded document management systems. Where a business is storing important records electronically, it will often be necessary to retain two electronic copies of the data, i.e. a primary copy and a back up copy.

**Alistair Wyvill, St Philips Chambers,
Birmingham**

As a barrister, Alistair Wyvill, regularly comes across electronic disclosure issues. Over the last five years, he has seen electronic documents go from being of marginal to critical importance in commercial litigation. How the parties agree to approach electronic disclosure at the start of litigation is therefore very important. As Alistair points out, this is one of the central themes of the electronic disclosure provision, and if not borne in mind at the outset and catered for appropriately in the protocol agreed by the parties, valuable forensic opportunities may be lost.

"...e-mail traffic is always a good starting point for a litigant looking for gold in another party's disclosure."

Alistair sees clients becoming slowly more aware of the risks (not just the benefits) of electronic communication. Most clients have by now had at least one experience where they have been

caught out by an electronic document, although some still have to learn. In one recent case, a witness had forgotten about the data trail stored on his computer . . . which didn't quite accord with his recollection of events.

A business's electronic records permit a litigant and the court to see almost all of that business's internal decision making processes, Alistair explains. Its computers will normally hold a permanent record of what at any point in time that business was "thinking" and who was doing that "thinking" for it. E-mail traffic will show the various views of management, and embedded and replicant data will show who created and amended key documents.

"...Falsification or even back-dating is easily exposed."

Back-up and "residual" data ("shadow" data left on a computer even after you think you have deleted it!) permit a litigant to recover documents which the party has attempted to destroy.

In Alistair's experience, e-mail traffic is always a good starting point for a litigant looking for gold in another party's disclosure. E-mails – particularly internal e-mails - are far closer in nature to conversational speech than formal correspondence. In a recent case, he and his solicitors discovered that critical e-mails had not been disclosed by the other side. Interestingly, this was not because the e-mails in question had been referred to elsewhere, but because they had not been produced at all! The usual 20 e-mails per day in relation to the relevant contract had mysteriously ceased two weeks before the critical decision. Plainly these "conversations" had not stopped; they were just too embarrassing for the party to reveal to its solicitors.

Alistair has also found computer records useful for checking the authenticity of documents. Falsification or even back-dating is easily exposed. And producing the primary electronic records or offering inspection of your client's IT



system by an independent expert is a good way of countering any allegation of falsification or back-dating by the other side.

Mark Carver, Vice President – Professional Liability, AIG Europe (UK) Limited

Mark Carver finds e-mail communication can cause a number of problems. People still treat e-mails as conversations, and it can be all too easy to dispatch a knee jerk response – especially if one is using a BlackBerry and typing in abbreviated text. Gone are the days when the natural delay between dictation and dispatch gave people a chance to amend what they might otherwise have sent in a fit of irritation. Then there is the informal way in which people often express themselves in e-mails. This can be embarrassing if the e-mails have to be disclosed, and enough to put one temporarily on the back foot in litigation.

"...Gone are the days when the natural delay between dictation and dispatch gave people a chance to amend what they might otherwise have sent in a fit of irritation."

Mark also sees the sheer volume and proliferation of e-mail communication as a problem: the curse of the 'cc' which promptly makes you debate whether to respond, and, even worse, the 'bcc' which means the recipient and open copyees are unaware of who else might have received the e-mail. And then attachments can cause difficulty too, for example

when they contain tracked changes which can be reinstated by the other side.

So far, electronic disclosure risk is not something which AIG Europe specifically factors into the calculation of professional indemnity premium, although Mark thinks this could change with the increasing use of the internet. However, AIG Europe does already ask clients whether they have internet and e-mail policies. It also holds an annual risk management conference which addresses internet and electronic communication issues, and sends out newsletters to clients on the subject twice a year.

So what steps would Mark advise clients to take to manage the risks inherent in electronic communication? Clear internet and e-mail policies, he says. And helpful points to cover in the e-mail policy? He comes up with a list: reminders to employees that corresponding by e-mail is the same as corresponding by letter, i.e. e-mails are documents; guidelines as to what communications should not be dealt with in e-mails, e.g. formal advice; a protocol for the format of e-mails; and suggestions for avoiding those knee-jerk responses!

And finally – some practical tips

- Have clear and comprehensive policies for internet and e-mail use, including an e-mail protocol.
- Have clear and comprehensive policies for document management and document retention, including a protocol for exiting staff.
- Keep a back up copy of any electronic records, and maintain, or have access to, the technology needed to retrieve data from superseded systems.
- Issue frequent reminders that e-mails (as well as other forms of electronic communication) are ‘documents’ which may be disclosable in the event of litigation.
- And a final tip - remember that computers store data trails of those ‘deleted’ documents! Your electronic brother is watching!



TLO Insurance Services Limited

Specialists in
Professional Indemnity Insurance

London
020 7839 0472

Hereford
01432 350657

Shrewsbury
01743 366350

Worcester
01905 729338

www.tloinsurance.co.uk

Authorised and regulated by the Financial Services Authority

TLO Insurance Services in association with Oliphant Consulting. © TLO Insurance Services Limited

This material is for general information only and is not intended to provide legal advice. In contributing to this article, the contributors are not acting on behalf of TLO Insurance Services, and any views expressed by the contributors are the contributors' own.