Is video-conferencing putting you at risk?

GRANT FEARY, DEPUTY DIRECTOR, LAW CLAIMS

It was not that long ago that video-conferencing was a new and expensive technology which was only available "at the big end of town" or in the Courts. Now of course, with the advent of Skype (and similar programs) and the ubiquity of smart phones, it is now possible to conduct video meetings easily and cheaply. Whilst the use of such technology can be of great assistance there are some real risks and practitioners need to bear these risks in mind so that they can be minimised.

From time to time the Society receives enquiries from practitioners about the use of video-conferencing in legal practice. Such enquiries have related to whether it can be used to witness documents, identify clients or give advice.

Law Claims is of the view that the witnessing of a signature should never be done via video-conferencing. An obvious difficulty is that the witness cannot be sure that the document sent to them to sign is the same document they saw being signed on the screen. A more fundamental problem, however, is the usual requirement in any witness clause that the person executing the document did so "*in the presence of*" the witness.

There is Canadian authority (*First Canadian Title Company Ltd v The Law Society of British Columbia 2004 BCSC 197*) that the witnessing of documents via video-conferencing did not satisfy the requirements for a lawyer to witness documents as an officer under the British Columbia Land Title Act. Whilst there is no direct Australian authority on the matter, it is difficult to see that any Court would find this requirement of the witness being "*in the presence* of " the person executing the document satisfied through a video-conference attendance.

As always, the question of the proper identity of your client looms large – you need to be satisfied that you are advising the right person. Reaching this level of satisfaction via video-conferencing will obviously be much harder (if not almost impossible) if you have not met the client before. Dealing with clients via video-conferencing should therefore generally only be done when you know the client well enough to be sure they are who they say they are.

Once you are satisfied as to your client's identity it may be just as, if not more convenient to give advice or receive instructions via video-conferencing, rather than over the telephone. It will not be as good as a face to face meeting though, especially if you need to go through documents.

Obviously, it is important to ensure that both you and your client can hear and see each other clearly and that the reception on both ends is clear and uninterrupted. It will also be important to know, and to remain apprised of at all times, whether there is anyone else in the room apart from your client who might influence them. It may not always be easy but it may be important to ensure that the client is alone, depending on the type of matter and advice to be given.

Video-conferencing software will also generally have the ability to record the meeting for later reference which may be helpful, both for you and the client. A recording should however only be made with the consent of all parties.

Consistent with our constant reminders to practitioners about cyber-security, the question of cyber-security as regards video-conferencing is also important. Video-conferencing equipment is extremely vulnerable to hackers. In the USA in 2012 a company specialising in cyber-security discovered 5,000 open conference rooms belonging to a range of businesses, including law firms, as a result of insecure video-conferencing systems. The company noted that businesses often invested large amounts of money in top quality video-conferencing facilities but set them up outside their computer firewalls, leaving the system open to attack. In the case of law firms the danger of inadvertent disclosure of confidential and privileged information is obvious.

The dangers don't stop there: even if your main office system is secure, lawyers working remotely (e.g. from home or in airports etc) via unsecured wireless networks are at risk. It may be that secure portable modems need to be employed.

As has been noted before in these pages, technology can be of great benefit to legal practices, as long as the relevant risks are also borne in mind.

VIDEO-CONFERENCING DO'S & DON'T'S

- Never witness signatures via video- conferencing
- Always take reasonable steps to properly identify your client
- New clients should always be identified in person
- Only give advice/take instructions if the audio and video reception is clear