Using New Technology for Remote Witnessing of Legal Documents in Victoria

Adam Darbyshire
The University of Melbourne, Australia

Paul Darbyshire
Victoria University, Australia

Abstract

Current legal requirements concerning the witnessing of affidavits and statutory declaration require the physical presence of both the authorised witness and the deponent. This can be time consuming process and seriously disadvantages people in remote rural areas and even those in urban areas with transport problems. Countries such as Australia with a low average population density and limited access to authorised witnesses will feel the effects of these limited laws to a greater degree. The current laws governing this process were developed for good reason, but recent technology advancements allow us to implement a witnessing method that does not require the physical proximity of either the deponent nor the witness. Current laws will not at this time permit this process, however, in this paper we outline a strategy for remote witnessing of documents that could be considered both secure and transparent for the legal process. This paper additionally presents the results of a survey undertaken to obtain comments from legal practitioners on this proposed method of remote witnessing.

Keywords

Agent, Communication, XML, Java, ACL, Architecture Framework

Introduction

Current legal requirements concerning the witnessing of affidavits and statutory declaration require the physical presence of both the authorised witness and the deponent. These requirements are contained in the Victorian 'Evidence Act' 1958, implied by the phrase 'in the presence of'. Affidavits and Statutory decelerations get their power as legal documents from the Evidence Act. Additionally, the administrative process for creating an Affidavit and Statutory Declaration is not specifically detailed in the Act, but has developed over time from the initial phrase detailed above from the Act.

The physical act of getting both the deponent and witness together can be time consuming in the best of circumstances. Add to this the fact Australia has a low population density with a large number of remote communities who are unable to easily obtain access to authorised witnesses. The current legal requirements outlined above also causes difficulty for people in areas with poor transport or those with disabilities that impede movement. The requirement for the physical presence of the witness and deponent was developed in a time when the current possibilities of technology could not be imagined. Current technology has developed to a point where a secure and transparent process for remote witnessing of legal documents can be implemented. Along with the technology component we need to develop a set of procedural steps to ensure the security and integrity of the witnessing process.

A high level overview of the remote witnessing process can be viewed in Figure 1. It is now possible to construct a procedural witnessing system to satisfy the general requirements of the 'in the presence of' clause in the current Act.

Figure 1 Possible new witness-deponent configuration

The technology solution makes use of the Internet, which is basically a global ubiquitous medium. The contribution of this paper is to provide a model for remote witnessing of documents utilising current technology. The model includes both a description of the required technology and configuration, as well as a set of procedures to be followed for using the technology configuration in order to maintain the integrity of the witnessing process. In the following sections, we provide a brief background of document witnessing, followed by a survey of legal professionals on the suitability and usability of remote witnessing. A brief analysis of this survey is provided. A detailed description of the technology configuration and set of procedural steps required to use the technology is given. Finally, conclusions and possibilities of further research are provided.

Background

Many aspects of the legal system have remained unchanged for hundreds of years. One aspect that has remained unchanged for some time is the process for witnessing documents. While there is a number of available documents outlining the procedural steps (Victorian parliament 2008), (Department of Justice (Victoria) 2005a), (Department of Justice (Victoria) 2005b), it is assumed that the deponent and witness will be together during the process. Although this may be the assumption in these documents, it is actually worded as 'in the presence of' in the Evidence Act 1958 (Victorian parliament 2008). This Act is what gives Statutory Declarations and Affidavits their legal authority. Additionally, the Evidence Act is the only place that dictates the requirements for the proximity of witness and deponent.

Butterworths Concise Australian Legal Dictionary defines presence as "The attendance, appearance, or existence of a person at a particular place at an identified time." (Butt 2004). This definition has served the traditional legal system well for many years before recent technological advancements. The original wording of the Evidence Act was constructed well before current technology provided us with any other possible alternative. In an environment where critical business meetings can occur with the participants never meeting face to face, it may be time to rethink the definition of the word presence. Particularly in relation to the clause '*in the presence of*'.

Recent changes and improvements to technology have provided methods for high quality audio visual communication over long distances (CISCO Systems 2009a). Indeed, as these technologies now utilise the Internet for communication, Long Distance can mean literally, anywhere. Technology similar to that which would be used in this proposed model has already been used by Australia's largest telecommunication provider Telstra, to project the presence of Telstra's chief technology officer Hugh Bradlow, over 700 kilometres for a business meeting (Reardon 2008).

Given that the only real interpretation requiring the presence of deponent and witness during the witnessing process is provided in the Evidence Act, there is a distinct lack of Literature attempting to redefine this requirement.

Survey and Analysis

Prior to the construction of a model for remote witnessing a survey was developed and sent to a number of legal practitioners in order to illicit the professional opinion of interested stakeholders. This was to help develop a set of procedural guidelines to maintain the integrity of the witnessing system. The survey was small and consisted of 10 open ended questions designed to obtain detailed responses. The survey questions are detailed below in Table 1.

Table 1: Survey questions

	What (Data)
1	What is your opinion of the possibility of honorary justices witnessing affidavits over large distances by Webcam?
2	Do you believe that electronically witnessed documents should be admissible in court?
3	Please list three to five of the major deponent identification requirements for a mote witnessing system.
4	Please list three to five potential challenges to the validity of remotely witnessed documents.
5	Please list three to five security requirements that you feel are important to ensure the security of an electronic witnessing system.
6	When a document is witnessed by a Webcam there are two versions of the document created with different signatures. Do you believe that a document electronically received by the Honorary Justice should become the original?
7	Do you believe a requirement should be that the data does not leave Australia?
8	Do you believe that to increase security a random number should be written on the top of the document to be witnessed to help improve security?
9	Do you believe that the document should not leave the field of vision of the camera for the entire duration of the witness
10	Would you believe a remote witnessing system that requires the following acceptable a) The data from the two computers never leaves Australia b) A random number being written on top of the page by the deponent at the time of witnessing c) The document never leaving the field of vision of the camera d) An identification system that requires the deponent to sign up for the remote witnessing service at a police station where a copy of their id is taken and digitised so the honorary justice can verify the deponents identity at the time of witness e) An electronic record of the video session and scanned document being recorded for verification of the procedure

The survey was sent to six legal professionals with five surveys returned. In most cases, the survey responses mirrored each other and a distillation of the responses is provided below:

1) All respondents believe that a remote witnessing system is potentially a good idea.
2) All respondents believe that a remotely witnessed documents should be admissible in court.
3) Most respondents have sighted the issue of providing 100 points of identification and the risk of fake ID, however one respondent believed there was no value in an identification system.
4) Out of the responses to this question, the following points were deemed the most important to the validity of the remote witnessing process.
   - Complying with signature requirements
   - Steps taken to prevent document tampering
   - How swearing on a religious book would be facilitated
   - Risk of forgery
   - Who has access to records to audit them
5) Out of the responses to this question, the following points were deemed the most important to the security of the remote witnessing process.
   - Recording sessions and documents
   - Recording details of the computer that the deponent is using
   - Privacy and security of stored information and ID
6) Respondents to this question were mixed but the majority of responses implied that the document that has been signed by the witness should become to original.
7) The majority of respondents did not see any value in ensuring the in-transit data remains in Australia.
8) The majority of the respondents stated that this or a more advanced form of document security should be a requirement.
9) The majority of the respondents stated that the document to be witnessed should remain inside the field of view of the camera at all times during the signing process.
10) All respondents to this question endorsed the idea of remote witnessing with the listed requirements as a framework.

The responses produced by the survey have provided significant information about what legal professionals consider important in a proposed remote witnessing system. A further analysis of some points from the survey responses follow:

Question 3: Please list of three to five of the major deponent identification requirements for a mote witnessing system.

The responses to this question covered issues regarding the amount of ID required and the validity of the ID which has to be used in the remote witnessing process.

A method around this is to have the deponent apply to get access to the remote witnessing system at their local police station. The police could verify identification of the deponent and then create an account for the deponent to be able to use the system.

Question 4: Please list three to five potential challenges to the validity of remotely witnessed documents.

The responses to this question were raising issues surrounding complying with legal requirements for sighting signatures, tampering with documents, auditing and the swearing process.

For sighting signatures, the most appropriate method for dealing with this is to ensure that the camera can focus on the pen as the deponent signs the document.

Tampering with documents on a remote witnessing system can be averted by keeping an electronic copy of the witnessed document on file with easy access by the courts. This process can be improved by ensuring that all deponents know that any document that they remotely witness will be stored on file for purposes including detection of altered documents.

Access to the witnessed documents should only be available to the courts and the deponent by application.

The swearing process for affidavits allows for a deponent to use a religious book, it would be in-practical for a witness to check the contents of a religious book over a Webcam to confirm its validity. For this reason it would be advisable to require that all affidavits are sworn by affirmation which does not require a religious book.

Question 5: Please list three to five security requirements that you feel are important to ensure the security of an electronic witnessing system.

The responses to this question mainly targeted access to the documents and files produced. Addressing all of the security requirements for a system may be excessive of work however all appropriate security measures must be taken to prevent access to the documents, recording and stored identification documents.

Question 6: When a document is witnessed by a Webcam there are two versions of the document created with different signatures. Do you believe that a document electronically received by the Honorary Justice should become the original?

The responses to this question were understandably mixed based on the training of the legal professional. The majority of responses that came back indicated that the signature of the authorised witness gives the document legal authority and is the preferred document to become the original.

Question 8: Do you believe that to increase security a random number should be written on the top of the document to be witnessed to help improve security?

The response to this question shows that there should be extra requirements on proving the authenticity of the documents. One such method is to instruct the deponent to leave a pre-determined marking on every page of the paper immediately before it is scanned and sent to the witness. An example of this would be the witness instructing the deponent to write the numbers ‘1234’ on top of the document they wish to be witnessed. The

deponent would then scan the document and send it to the witness who would then confirm that the number written on the received document matches the number that the deponent was instructed to write. This is an added step to further show the authenticity of the document that has been received by the witness.

Remote Witnessing Technology

With the recent advances in technology it is now possible to maintain a video and audio link between two locations using the Internet as a communications medium. The technology configuration required for the proposed Remote Witnessing process is shown below in Figure 2.

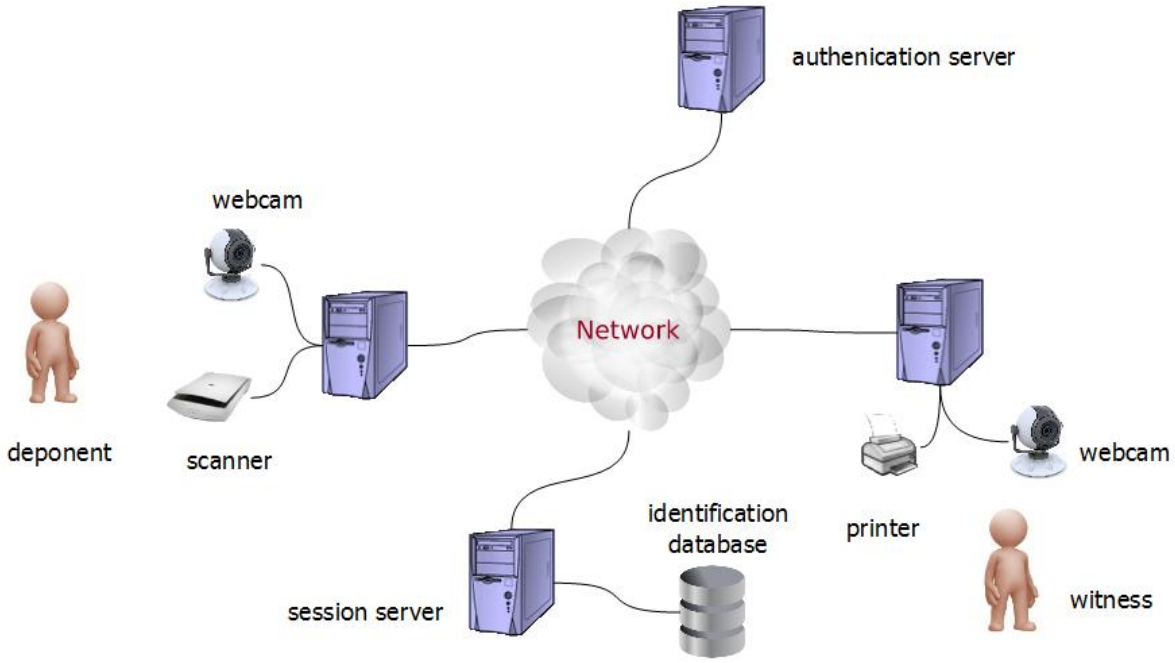

Figure 2 Possible new witness-deponent configuration

The major components shown in Figure 2 are:

- **Deponent Local System**
  This is the local system of the deponent. This system must have Broadband Internet access, as well as a scanner, Webcam and microphone.
- **Witness Local System**
  The local system for the witness. This system must have Broadband Internet access, as well as a printer, Webcam and microphone.
- **Session Server**
  The session server is used as an intermediary between the deponent and witness's computers, this facilitates third party recording of aspects the remote witnessing process from video and audio to the document that was to be witnessed.
- **Identification Database**
  The identification database contains electronic copies of the ID required for a witness to identify a deponent.
- **Authentication Server**
  The authentication server contains the user accounts which will be required to login to the software for the process.
- **Internet**
  The Internet becomes the medium via which the witness extends their presence to the deponent. As the Internet has developed into a global ubiquitous communication medium since the mid

1990's, this becomes the most cost effective and available communication channel for remote witnessing.

The Webcams and microphones become a critical component of the remote witnessing technology as together they allow us to achieve the essence of the '*in the presence of*' clause of the Evidence Act.

Software

Specialist software which is designed to support the remote witnessing process would need to be commissioned. The ideal software for this process would come in three parts to be able to perform as an effective framework for a procedural model to be fully developed.

The deponent would require a software client on their local computer that presents them with a simple method of communicating with the witness and exchanging the appropriate documents.

The witness will require a second software client that appears similar to the deponents client however, it will need specialised functionality to assist the witness. Some of the extra functionality that would be needed is to present the witness with electronic copies of identification as well as an administrative function to notify the appropriate staff when identification documents do not appear to match the deponent.

A software package that will seamlessly handle the communication process from both ends including recording functions while being a secure system.

Security

Security is a critical component to a system that has personal identifying documents stored electronically. The security of a remote witnessing system would have to be extremely well designed and monitored constantly.

Some security recommendations would be:

1) Encrypted hard drives
2) Stress tested programs
3) Encrypted communications
4) Database with multiple levels of access
5) Redundant storage to protect data
6) Frequent security audits
7) Significant user training
8) Virtual private networks
9) OS hardening

Procedural Steps for Remote Witnessing

The technology for remote witnessing discussed in the previous section only facilitates the procedural steps required to maintain the integrity of a remote witnessing process. The procedural steps have been designed to maintain the same level of transparent authenticity as that of the traditional witnessing process, with video records. The survey responses detailed in a previous section have provided valuable input from current legal practitioners in refining the following procedural steps as a necessary component for this model of remote witnessing.

1) Deponent will register for the remote witnessing system at a local Police Station.

   This will allow checking of the deponents identification which can then be entered into the ID Database which will be available to an authorised witness at the appropriate times.

   This step would only need to be completed on initial registration to the remote witnessing system and when the ID which is electronically stored expires.

2) Deponent launches software to connect to the server
3) Deponent automatically joins a queue that will connect them to the first available witness

4) Witness launches software to connect to the session server
5) Witness and Deponent are connected to each other.

   The witness and deponent are connected to each other to begin the witnessing process.

6) Witness identifies the Deponent

   The witness is provided with electronic scanned copies of the deponents ID which the witness can then use to confirm the deponents' identity.

7) Deponent performs the affirmation

   The deponent would perform the affirmation instead of swearing on a holy book as it lowers administrative overhead.

8) Deponent signs the document in the appropriate place

   As per traditional witnessing of documents the deponent signs the document within the electronic presence of the witness.

9) Witness provides a random number to be written at the top of every page

   The witness will provide the deponent with a random number that is generated by the program which will be written on top of every page to be signed by the witness. This is to add to the security of the process to show that the document received by the witness is without a doubt the one signed by the deponent.

10) The document is then scanned by the deponent and sent to the witness

    The deponent would place the documents to be scanned in their scanner and the program would scan and send the documents to the witness to be printed.

11) The witness would then confirm the authenticity of the documents.

    The witness would print the documents and confirm that the documents are the correct ones by checking the random number that was to be written on the top of the documents as well compare the signature on the document to that on any electronic ID.

12) The witness would sign and pass the documents on

    On the condition that the witness is satisfied that the documents are authentic the witness would then sign the documents which then become the original and passed on accordingly.

13) Recording keeping

    The process above would be recorded and placed in a suitable location to allow appropriate authorities to audit the process if it was ever questioned later.

Conclusion

This paper has presented a model for remote witnessing of legal documents. A model such as this will necessarily contain two major components: the technology component; and then a set of procedural steps to be followed.

The survey presented above provided a brief insight into the mind set of legal professionals. While only a small number of surveys were sent out the detailed responses provided an exemplary source of information. The detailed responses have helped provide a suitable framework on which to develop a set of technological and procedural requirements.

The technology component would involve having an appropriate hardware set-up on both the witness and deponents computers, as well as a set of servers to assist witnesses in performing critical background tasks such as witness identification. The final section of the technology component would be the end user software that will integrate all aspects of the process into a simple interface.

The procedural component of the remote witnessing process will involve a set of clearly defined steps which must be followed for a document to be valid. The finalised procedural methodology will be the subject to scrutiny and subsequently must be well refined and well tested.

Further Research and work

The development of a model for remote witnessing is just the beginning of a long process to realisation. Further research will be required in a number of areas including, legal interpretation for the clause 'in the presence of', political and public opinion and comment of the model, professional critical evaluation, as well as further investigation in to security and privacy issues.

References

Arenson, K.J. & Bagaric, M., 2007. *Rules of evidence in Australia Text & Cases* Second., Chatswood, NSW, Australia: Lexis Nexis Butterworths.

Bates, F., 1985. *Principles of Evidence* Third., North Ryde, NSW, Australia: The Law Book Company.

Beer, S., 2008. Telstra: may the holographic force be with you! Available at: http://www.itwire.com/content/view/18458/1231/ [Accessed September 30, 2009].

Brien, C. & Brien, J., 2004. *NetLaw*, Lexis Nexis Butterworths.

Butt, P. ed., 2004. Butterworths Concise Australian Legal Dictionary. In Reed International Books Australia.

Casey, E., 2004. *Digital evidence and Computer crime: Forensic Science, Computers and the Internet* Second., London: Elsevier Academic Press. Available at: 0-12-163104-4.

CISCO Systems, 2009a. Cisco Introduces Personal TelePresence. Available at: http://newsroom.cisco.com/dlls/2008/prod_051208b.html [Accessed September 30, 2009].

CISCO Systems, 2009b. Overview Telepresence. Available at: http://www.cisco.com/en/US/netsol/ns669/networking_solutions_solution_segment_home.html [Accessed September 30, 2009].

Dapzury, V. & Shrivastava, P., 2002. Interview as a Method for Qualitative Research. Available at: http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf [Accessed September 30, 2009].

Department of Justice(Victoria), 2005a. Guidelines for Authorised Witnesses.

Department of Justice(Victoria), 2005b. Witnessing of Documents.

Fen Lim, Y., 2007. *Cyberspace Law commentaries and materials* Second., Oxford University Press.

Keane, A., 2006. *The modern law of evidence* Second., Oxford University Press.

Moir, E., 1969. *British Institutions The Justice of the Peace*, Pelican.

Reardon, M., 2008. Beam me up, Telstra. Available at: http://news.cnet.com/8301-10784_3-9955821-7.html [Accessed September 30, 2009].

Stokrocki, M., Qualitative Interview Method. Available at: http://www.public.asu.edu/~ifmls/artinculturalcontextsfolder/qualintermeth.html [Accessed August 3, 2009].

Dapzury, V. & Shrivastava, P., 2002. Interview as a Method forResearch. Available at: http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf [Accessed August 3, 2009].

Victorian parliament, 2008. *EVIDENCE ACT 1958 (Vic) s 99-126.*,