LAW IN ORDER

CASE STUDY

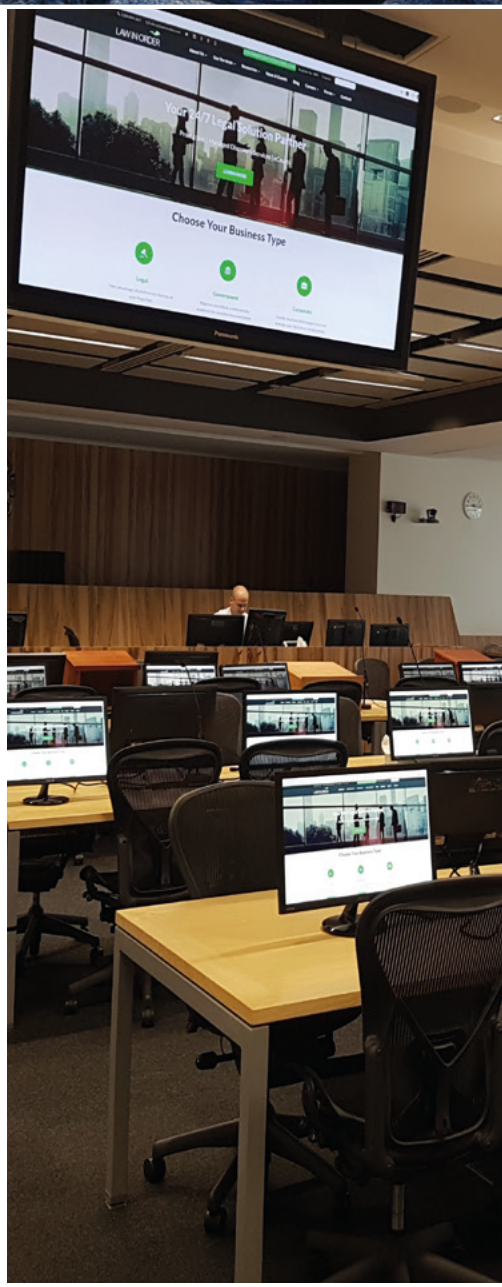
Managing Confidentiality in a Virtual Trial

The Challenge

Law In Order were approached by the law firms involved in a high profile case to determine whether we could assist facilitating an eTrial. The matter was proposed to be conducted either virtually, hybrid or in-person depending on the circumstances at the time. The case presented various complexities surrounding the management of confidential evidence and the COVID-19 related travel restrictions imposed on lawyers and witnesses involved in the matter. Lawyers and witnesses required the ability to appear from various Australian state locations and within an Australian Supreme Court that also had restrictions on who could access the hearing so it was determined that a video call would be required for the hearing.

To ensure we could adequately manage the requirements for this matter, considerations were required for the following complexities:

- **COVID-19 Restrictions**
  Managing their impact on any element of service.
- **Videoconference Call**
  How to manage the various virtual attendees in the virtual hearing with varying levels of confidentiality applied to the evidence, without disrupting the proceeding.
- **Evidence Presentation**
  How to manage confidential document display in a virtual setting.
- **Evidence Management/Online Court Book**
  How to manage the confidential documents across the online court book.
- **Webstream**
  How to manage the principle of open justice with a public webstream of the hearing, while preserving confidentiality of the proceeding when required.



Our Solution

Virtual/Hybrid Trial

The concern involving travel restrictions imposed on lawyers and witnesses was alleviated by designating a virtual/hybrid trial using videoconferencing platforms, allowing legal teams and witnesses to appear from their firm, chambers or home with the Judge and Associate connecting from the court. The witnesses would appear from either a party's law firm if convenient or their home. Rigorous testing was conducted with all relevant parties and the court to ensure sufficient stability was available with this approach. Firms connected from New South Wales, Victoria and Western Australia with witnesses connecting from across Australia.

Separate Video Conference Links

The complexity surrounding management of the videoconference platform (VC) was resolved by facilitating two separate VC links. One link designated for the video call (Link A) and a second link for the evidence presentation/document display (Link B). By using a separate link for the Evidence (Link B), it enables complete control over who can review the documents, when confidentiality restrictions apply to a particular document displayed on Link B. A virtual participant's access to this is managed in real-time by the Bridge Manager (the VC Bridge operator who manages the virtual hearing) by transferring the participants not permitted to view that document to a breakout room until the examination concerning that document is complete, then returning those participants to the main room of the VC link.

The VC platforms are managed by a dedicated Bridge Manager, who is responsible for managing the virtual hearing platforms and the integrations of other elements of the service such as Evidence Presentation and Webstreaming. Our experienced Bridge Managers combine their technology expertise with their legal knowledge to provide optimal management of virtual/ hybrid hearings. They provide real-time remote technical support for all online components of a virtual matter and their responsibilities include:

- Virtual lobby admissions
- Monitoring approved attendees to ensure the permitted participants can access the trial while preserving the security of restricted sessions
- Managing break out rooms for legal teams and witnesses as required
- Remote technical support of the VC platform
- Ensuring all core participants are visible and observing participants do not disrupt the hearing
- Maintaining ongoing communication with updates or advice for all participants pursuant to the instructions of the court or the parties

The bridge manager has complete control over who is permitted for each Link, whether it is regrading the Video Link A or the Evidence Link B. When witnesses are to appear, prior to their appearance they will be kept in a breakout room, they will not be able to enter the virtual hearing or hear any discussion of the matter until the court deems it appropriate that they can join the call. When this instruction is received, the Bridge Manager will transfer the witness into the main call of the hearing. This is the same process conducted when removing participants from legal teams that are not privy to the confidential documents at the time. Participants can be removed from only Link B, if it is permitted that the person still remain in the hearing but can't see the document Alternatively they can be removed from both Link A and Link B, if hearing discussion of the document is also restricted. We are flexible with our approach and can adapt to shifting requirements as the matter proceeds and instructions change.

Protocol for the Video Conference Platforms

Third, the complexity of managing confidential document display in a virtual hearing is resolved by adopting a rigorous protocol for the VC platforms and monitoring permissions of virtual attendees, removing participants without permission for different levels of confidentiality. This is supported by strong communication between the Evidence Presentation Operator and Bridge Manager to coordinate these ongoing changes. All documents in the court book include their respective confidentiality level assigned and noted in the metadata of the document. This information is also included in a column of the court book index. That way, when a document is called for display, the Evidence Operator communicates the permission level of that document to the Bridge Manager, who will then move the unpermitted participants for that level of confidentiality to a breakout room, then immediately confirm when this has been actioned to the Evidence Operator before displaying the document for the permitted participants. An approved participant list is kept by all Law In Order personnel engaged in the matter and this document details each participant's approval to join the hearing and what respective permission they have in terms of accessing the virtual hearing and accessing the display of documents.

Secure Servers and Confidentiality Agreements

Fourth, the digital court book and related evidence management of confidential documents was conducted in accordance with our standard practice followed in any Law In Order eHearings matter to ensure the data is stored on secure servers and managed by permitted staff. Law In Order and its employees take the security and protection of client data and information seriously and ensure confidential client information and evidence databases pertaining to live/active matters are protected. All staff working on the matter signed confidentiality agreements provided by the parties and only those staff members were permitted to support the operation.

All data related to any eHearings matter is stored on AUCloud servers, which are IRAP certified and the preferred servers of the Australian Government. AUCloud is Australia's sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on the Australian Government, Defence, Intelligence and Critical National Industry (CNI) communities. All our data is stored on these servers which are Australian owned, managed and operated with all data and services sovereign, resident, monitored and operated in Australia by Australian citizens.

Public Webstream Protocol

Fifth, the public webstream of the hearing is used to support the principle of open justice. Given the nature of confidentiality that sessions may require, we have a rigid protocol the Webcast Operator follows for managing open and closed court sessions, preserving confidentiality of the proceeding when required. Link A is the only link ever used for webstreaming the proceeding where confidential documents are involved. That way no document that is a part of the virtual hearing will ever appear on a webstream. Only the videos and audio of people visible on Link A will be used for a public webcast. We have extensive experience managing confidentiality of sensitive or protected evidence during public or private hearings that are webcast. This includes discussions of substance related to a document that is not seen. We manage this by applying redactions to audio and/or video when content is confidential or protected by Public Interest Immunity, Suppression Orders, Non-Publication Orders or Pseudonym Orders, or switching between open and closed webstream sessions. These changes are applied in real-time and at the instruction of the court or the parties. When the court moved into a section of the examination that dealt with a document covered by a level of confidentiality, we would mute the webcast audio and video with a closed court banner to indicate this. When the session returns to being open to the public, we revert to the open webstream. All these changes are instructed by the court or the parties and applied in real-time. A delay is also applied to the stream, to enable greater control over any redactions that may be realised after they happen although this is limited to a two-minute delay.

The Outcome

The matter commenced early September 2021 and is ongoing in an Australian Supreme Court Jurisdiction with parties and witnesses connecting to the virtual eTrial from New South Wales, Victoria and Western Australia. All firms are located in states that were restricted to travel and the virtual format of this trial has been suitable for all involved. All witnesses have been managed successfully and no one has been disadvantaged by virtual appearances. The management of the confidential documents for Evidence Presentation and the Digital Court Book has been conducted efficiently with the court's expectations and the parties' specific requirements. The matter has been conducted successfully and there have been no breaches of security.