Law Society of Saskatchewan

Practice Resource

Video Conferencing Technology: Guidance and Professional Obligations

Introduction

In recent years, the use of video conferencing technology by law firms and lawyers has become common practice, from providing legal services to holding meetings with clients or law firm staff. When contemplating or using video conferencing, consider which products and platforms work well for meetings with clients and other lawyers and law firm staff, while maintaining client confidentiality and security of records. The effective use of technology is an essential part of responsible legal practice.

Is Video Conferencing the Best Option in the Circumstance?

Although many video conferencing products include security settings such as end-to-end encryption that may prevent hacking, users are often left with little to no security training to configure these settings. It is recommended to have an information technology professional assist with setting up video conferencing technology. Note the professional obligations in the Code of Professional Conduct (Code) rule 3.1-2, commentary [4A] and [4B] regarding technological competence:

> [4A] To maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3.
>
> [4B] The required level of technological competence will depend upon whether the use or understanding of technology is necessary to the nature and area of the lawyer's practice and responsibilities and whether the relevant technology is reasonably available to the lawyer. In determining whether technology is reasonably available, consideration should be given to factors including:
>
> a) the lawyer's or law firm's practice areas;
> b) the geographic locations of the lawyer's or firm's practice; and
> c) the requirements of clients.

The appropriate degree of security for the situation will depend upon the nature of the conversations and business being transacted. Even with virtual transactions, Code rule 3.2-1 applies. Commentary [3] states that what is effective communication will vary depending on the nature of the retainer, the needs and sophistication of the client and the need for the client to make fully informed decisions and provide instructions.

If the conversation is of a deeply sensitive nature, confidentiality and security may be better achieved with a phone call than a video call. Conversely, if the purpose of the video call is a social check-in with an employee, it is reasonable to be less concerned about a video call. Many video calls fall somewhere between the two scenarios outlined. For example, while the plan

may be to call a client to check how they are managing their business, the client may move from giving a general summary to seeking advice or services about a particular problem. Consider what is intended to be discussed, whether that conversation is confidential or privileged and seek software with sufficiently robust security features. Features legal professionals may want to include are:

- End-to-end encryption;
- Ability to set up a meeting identification, which is randomized and is assigned to each meeting to keep credentials private;
- Ability to set up participant passcodes, which are a second level of authentication that can be enabled for each meeting;
- A way for the host to lock the meeting;
- A way to expel participants; and
- Waiting room features which allow participants to wait in a separate virtual room before the meeting and allow the host to admit only people who are supposed to be in the room.

In addition, use a firewall to prevent unauthorized network traffic from reaching devices, and always make sure to use the latest version.

Whether working from the office or remotely, it is important to arrange an appropriate space for confidential communications generally and for video conferencing (Code rule 3.3-1). Consider how to keep client and other confidential information protected by:

- Working in a private area;
- Protecting passwords and locking devices if left unattended; and
- Ensuring there is a space for taking calls where conversations will not be overheard

Ensure reasonable security arrangements against all risks of loss, destruction, and unauthorized access, use or disclosure of records related to practice and the information contained in them.

Selecting a Service Provider

There are several video conferencing products including Skype for Business, Zoom One, Amazon Chime, Microsoft Teams, Webexby Cisco, TeamViewer, GoToMeeting, Signal, Jabber, Google Meet and the ones associated with particular operating systems, such as Facetime and WhatsApp. Each has different advantages and disadvantages. Some support more than 100 participants. Some, but not all, offer end-to-end encryption that is difficult to hack.

The Law Society does not endorse particular products or service providers. This Practice Resource is intended to provide background information that helps meet professional obligations.

Many video conferencing tools use cloud-based services. The Law Society's Cloud Computing Guide can help determine whether a product complies with Law Society requirements. Responses to the questions in the guide can often be answered by reviewing publicly available sources and the service provider's terms of service.

Consider using enterprise software (rather than personal, consumer-grade) for client meetings and internal meetings where clients and their representation are discussed. Consumer tools may not have all the administrative and security tools needed to ensure that the conference is private. Although no video conferencing product can guarantee complete protection from threats, a more

complete set of security tools is likely with products geared for enterprise use.

Best Practices for Video Conferencing

When using video conferencing for the provision of legal advice or services, adopt these best practices:

- Advise the client not to share links with anyone else;
- Access links through a secured Wi-Fi network;
- Confirm the client's consent to proceed in this manner;
- Ask that all individuals in the remote location introduce themselves;
- Ensure no one else is at the remote location who may be improperly influencing the client;
- Make sure that audio and video feeds are stable and that all parties can be heard and seen;
- Manage screen sharing as the host and do not allow clients to screen share by default;
- Lock the meeting once the client or clients have joined the conference;
- Determine how to provide the client with copies of documents executed remotely;
- Confirm the client's understanding about the documents they are executing and provide adequate opportunity to ask questions during the video conference;
- Maintain detailed records including: date, start and end time, method of communication, identity of all present, and minutes of the content of the meeting; and
- If using video conferencing in completing client verification requirements, please refer to the procedures outlined in the Law Society's Practice Resource Virtual Verification of Client Identity Using Authentication Technology.

Many products provide the ability to record a video conference meeting, and as part of maintaining detailed records, consider recording the conversation with a client, with their consent. Ensure compliance with Code rule 7.2-3 which states that a lawyer must not use any device to record a conversation between the lawyer and a client or another lawyer, even if lawful, without first informing the other person of the intention to do so.

Questions

Contact tech-help@lawsociety.sk.ca to discuss specific issues regarding video conferencing.