Law Society
of British Columbia

Practice Resource

Using video-conferencing technology: guidance and professional obligations

v. 2.0 [updated April 2024]

Introduction

Many law firms and lawyers made a rapid transition to providing some legal services and holding internal meetings virtually by using video-conferencing technology during the COVID 19 pandemic. Since then, holding meetings with clients and law firm staff via video-conferencing is common. If you are thinking of using video conferencing, consider which videoconferencing products and platforms work well for meetings with clients, 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 circumstances?

There have been media reports about the security (or lack thereof) of video conferencing. It can be hard to know how to keep meetings secure. Although many video-conferencing products include security settings such as end-to-end encryption that may prevent hacking, often users are left with little to no security training to configure these settings. If technology is not your forte, it is a good idea to have an information technology professional assist you with setting things up. Note your professional obligations in *BC Code* rule 3.1-2, commentary [4.1] and [4.2] regarding technological competence:

> [4.1] 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.

> [4.2] 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 your situation will depend upon the nature of the conversations and business you are transacting. Even with virtual transactions, *Code* rule 3.2-1 applies. Commentary [3] to the rule 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.

In any event, if the conversation to be had 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, a lawyer may reasonably be less concerned about making a video call.

Many video-calls fall somewhere between the two scenarios outlined above. For example, while you may have planned to call a client just to check in about how they are managing their business through the current pandemic, the client may move from giving a general summary to seeking advice or services about a particular problem. Consider what you intend to discuss, and whether that conversation is confidential or privileged, and seek a software with sufficiently robust security features. Features lawyers may want include:

- End-to-end encryption;
- Ability to set up a meeting ID, 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;

- 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 to the above, use a firewall to prevent unauthorized network traffic from reaching your devices, and always make sure that you use the latest version of the operating system you have chosen to video conference your clients.

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 cannot endorse particular products. Our goal is to provide you with background information that helps you to choose what works best for you.

Many video-conferencing tools engage cloud-based services. The Cloud Computing Checklist can help you determine whether a product is compliant with the Law Society's requirements. Answers to the questions in the checklist can often be answered by reviewing publicly available sources and the service provider's terms of service.

Consider using an enterprise software (rather than personal, consumer-grade) for client meetings and internal meetings within which you discuss clients and their representation. Consumer tools may not have all the administrative and security tools you need to ensure that your conference is private. Although no video-conferencing service can guarantee 100% protection from threats, you are much more likely to get a more complete set of security tools with products geared for enterprise use.

Best practices for video-conferencing

When using video-conferencing for the provision of legal advice or services, lawyers should:

- Advise the client not to share the links with anyone else;
- Access the 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 you can hear and see all parties;
- Do not allow clients to screen share by default. As the host you should be able to manage the screen sharing;
- Lock the meeting once the client or clients have joined the conference;
- Where government-issued photo ID is produced to support verification of identity, use reliable authentication technology. Read the practice resource, Guidance for virtual verification of your client's identity using government-issued photo ID and technology) Ensure that a copy of the identity document (front and back) is sent to you in advance of your video meeting (consider requesting high resolution) and that when it is produced during the meeting the entire document is visible and legible;
- Determine how to provide the client with copies of the document executed remotely;
- Confirm your client's understanding about the documents they are executing and provide adequate opportunity for them to ask questions during the video conference; and
- Maintain detailed records including: date, start and end time, method of communication, identity of all present, and minutes of content of meeting.

Many products provide the ability to record a video-conference meeting, and as part of maintaining detailed records, you may think about recording the conversation between you and your client. Ensure you abide by *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.

Setting up a home office

You may be thinking of setting up a home office. It is important to set up 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 from family members and others. The conditions you look for in your home office or remote workplace should include:

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

The Office of the Information and Privacy Commissioner for British Columbia ("OIPCBC") developed a guidance document, Protecting Personal Information Away from the Office (January 2015) that provides common-sense steps and tips on how to keep information secure when working remotely. The Law Society's practice resource, Lawyers Sharing Space, offers tips and information about sharing space with people who are not lawyers.

Ensure that you have made reasonable security arrangements against all risks of loss, destruction, and unauthorized access, use or disclosure of your records related to your practice and the information contained in them (Law Society Rule 10-4). Take steps to put into place technological, physical, and organizational safeguards specific to working from home for you and your staff. You can test your home or remote office set-up by using the OIPC BC's self-assessment tool, Securing Personal Information (October 2020) in regard to establishing and maintaining reasonable security arrangements.

Indemnity and insurance

Review LIF's risk management tips for video-conferencing to reduce the risk of a negligence claim.

Questions

If you would like to discuss a specific issue regarding video-conferencing, lawyers are welcome to contact a Practice Advisor by email or phone (practiceadvice@lsbc.org or 604.443.5797) or to book an appointment.