BAMBOO
DATA CONSULTING

Ontario Trial Lawyers Association

Video Conferencing: A Guide to Litigate in a Secure and Private Manner

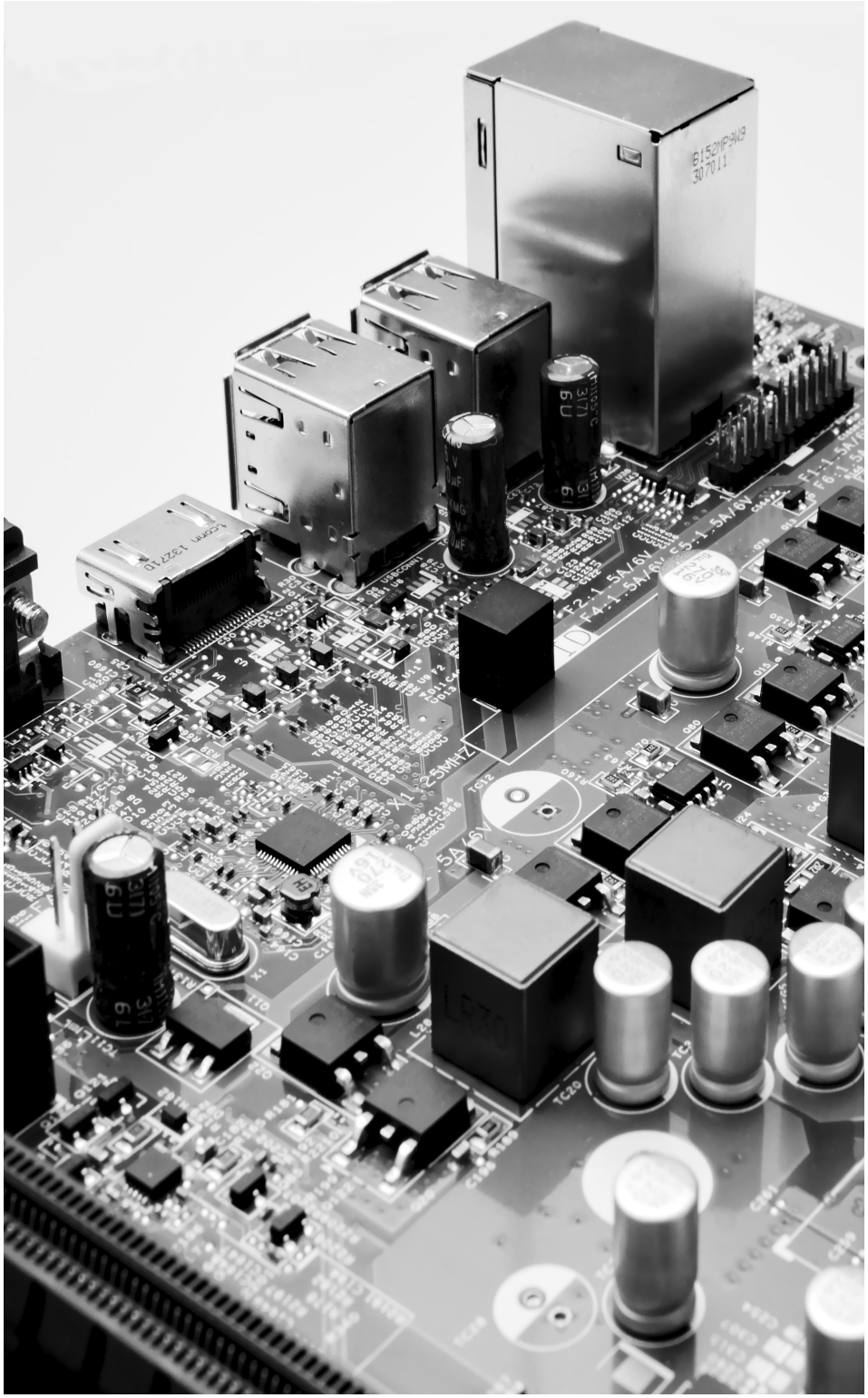
CONFIDENTIAL

May 2020

"…in 2020, use of readily available technology is part of the basic skillset required of civil litigators and courts.

- Justice F. L. Myers
Arconti et al v. Smith, 2020 ONSC 2782

Table of Contents.



Executive Overview.

Lawyers are working remotely in light of the current pandemic crisis and as a result implementing technological solutions, such as video conferencing to maintain their practice and service their clients with as little disruption as possible.

The use of technology can have indisputable benefits to the legal industry, which is often viewed of as 'archaic'. Many lawyers have discovered that litigation can be practiced in a more time efficient and cost-effective way through the use of technology. Similarly, courts and other legal institutions have been open minded and have implemented modern approaches to enable access to justice for litigants.

While there are risks associated with the use of technology, these risks can be effectively managed. The legal industry should seize this opportunity and bring about technological advancements that are long overdue.

As with any new practice models, risks need to be identified and inherent harm must be evaluated. Practices to mitigate harm must be designed so that residual harm, if any, can be minimized.

90% of legal professionals believe they need to do more to show employees and consumers they are protecting personal data

(2019 Data Protection Report, Shred-It)

Privacy and security risks are inherent in the use of technology, including video conferencing. There has been an uptake in privacy and security breaches, as more businesses and institutions have transitioned to online technologies to continue their practice remotely. This increase in breaches has resulted in class action lawsuits, regulatory investigations, remediation costs, and reputational harm.

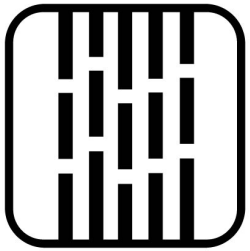
These breaches are, however, largely due to the lack of preparedness on the part of businesses including a lack of accountability/governance, a lack of policies and procedures, a lack of staff training, a lack of technological and administrative tools to assist in identifying vulnerabilities, and a lack of cyber insurance. These breaches can be effectively managed.

Prior to the pandemic, video conferencing was not used widely by the legal sector, despite the *Rules of Civil Procedure* allowing for the use of video conferencing in court proceedings. According to the *Rules*, parties must agree and/or be ordered by the presiding judge to use video conferencing, after evaluating objections. One objection currently being raised (mostly by insurers) is the lack of security of video conference platforms. This objection can be effectively managed if all parties implement strong privacy and security practices, as required by the *Rules of Professional Conduct,* LawPro, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

If law firms and insurers take a proactive approach to protect their clients' personal information from unauthorized access, risks can be effectively managed and law firms, insurers and the courts can benefit from the modernized and practical way of convening litigation.

This Guide is meant to identify a law firm's obligation to protect its clients' personal information while engaging in a video conference call. Recommendations are outlined to enhance the law firm's privacy and security posture and effectively minimize the risk of a breach.

About Bamboo Data Consulting.



Trusted Leaders. Passionate Collaborators.

Sharon Bauer is the founder of Bamboo Data Consulting, a consulting firm specializing in privacy, security, data strategy and a range of cutting-edge technology ethics work. Bamboo Data Consulting was founded to help businesses, government and non-profit organizations meet their strategic business goals by using data in a responsible and ethical way.

Bamboo Data Consulting enables growth, innovation, and transformation by bringing expertise to privacy and security solutions to ensure compliance with regulations, standards and best practices.

Sharon is a privacy consultant and lawyer. She provides strategic risk management and privacy compliance advisory and legal services. Sharon works with diverse private and public organizations, from startups to multinational corporations in industries such as technology, financial services, telecommunication, healthcare, education, marketing, and retail.

Sharon frequently conducts privacy risk assessments against international privacy legislations such as PIPEDA, GDPR, HIPAA, and CCPA to identify privacy gaps and make recommendations for remediation. She designs and implements privacy programs, including policies, compliance plans, and staff training programs. She conducts vendor privacy due diligence and data reviews in preparation for mergers and acquisitions. Sharon acts as a virtual Chief Privacy Officer for various organization where she provides ongoing privacy advisory services.

Prior to founding Bamboo Data Consulting, Sharon was a senior manager at KPMG where she led the national privacy team and developed the Privacy by Design Certification Program. Sharon assisted multiple multinational companies embed privacy practices into their processes, services, and products for the purpose of being certified by an accredited body.

Sharon started her career as an insurance litigator for 10 years representing plaintiffs.

Sharon frequently speaks and publishes on emerging privacy trends and technologies. She has taught courses on Canadian privacy legislation and Privacy by Design. She frequently contributes to The Lawyer's Daily on privacy matters.

Video Conference Lifecycle.

Embedding privacy and security into virtual litigation

ONE

Getting Started

Conduct due diligence on video conference service providers and implement privacy and security management / accountability within the law firm.

TWO

Setting Up

Set appropriate default settings on the video conference platform and develop privacy and security best practices for video conferencing.

THREE

Starting a Video Conference

Set expectations upfront about privacy and security so all parties are informed and can provide meaningful consent.

FOUR

During a Video Conference

Monitor and maintain privacy and security throughout the video conference call.

FIVE

Ending a Video Conference / Post Video Conference

Take extra precaution to ensure the video conference ended and securely protect any recordings.

SIX

Breach Preparedness

Privacy and security is never guaranteed; be proactive and mitigate the harm to both clients and the law firm.

Getting Started.

Conduct due diligence on video conference service providers and implement privacy and security management/accountability within your law firm

Review Agreements & Privacy Policies

As a law firm, you are the custodian of your clients' sensitive personal information and therefore have a responsibility to protect it. When engaging with third parties, vendors or service providers ("Vendors"), such as video conference Vendors, you must conduct due diligence on the Vendor to investigate whether it has appropriate privacy and security safeguards in place to protect your clients' personal information. *While you may outsource processes and services to Vendors, you cannot outsource your responsibility to protect the personal information your clients entrust you with*. Therefore, if a Vendor experiences a breach involving the personal information you disclosed to it, your law firm may be liable.

33% of breaches are a result of vendor breaches (Beazley, 2017)

When negotiating/reviewing service agreements, (a) limit the way in which the Vendor may use the personal information, (b) limit who the Vendor can disclose the information to (e.g. fourth party vendors), and (c) limit how long the Vendor may retain the information. Make sure the Vendor has appropriate privacy and security safeguards (e.g. certifications, attestations) to protect the personal information and, if possible, ensure the Vendor stores the personal information in Canada. If the personal information is stored outside of Canada, you must inform your clients that their personal information will reside in a different jurisdiction and the laws of that jurisdiction will govern their personal information.

Recommendations:

- ❑ Although it may not always be possible to negotiate video conference licensing agreements, to protect your clients' personal information, be aware of the following provisions in the licensing agreement or identify them within the Vendor's Privacy Policy:
    - How will the platform use personal information?
    - Who will the platform share personal information with?
    - Where will the personal information be stored or processed?
    - How long will the platform retain personal information?
    - How can an individual access their personal information?

Getting Started.

Conduct due diligence on video conference service providers and implement privacy and security management/accountability within your law firm

Develop / Re-Visit Your Privacy Policies

Video conference calls allow you to collect personal information that you otherwise may not have collected, such as images of the call, visual recordings and audio recordings. Law firms may collect personal information that they otherwise would not have collected but for video conferencing (e.g. audio recordings). Review your Privacy Policy (or Retainer Agreements) to ensure it addresses the collection of the newly acquired personal information and the way in which you intend to use it. As a precaution, seek meaningful and informed consent (e.g. signed Consent Form) from clients to engage in video conference calls and provide them notice of the risks such as privacy breaches or that their personal information may be governed by the laws of a different jurisdiction. The Office of the Privacy Commissioner of Canada (OPC) provides guidance on preparing Privacy Policies in order to rely on informed and meaningful consent (https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/02_05_d_56_tips2/).

Law firms should develop written and formalized internal policies and procedures to address privacy and security (e.g. Work From Home Policy, Clean Desk Policy, Internal Privacy Policy, Retention Policy, Electronic Communication Policy), which are accessible to all staff and provide clarity, uniformity and accountability towards the implementation of privacy practices.

Staff should be trained on internal privacy procedures, including their responsibility to protect clients' personal information. Staff should also be trained to identify and report a privacy breach and be educated on ways to avoid being a victim to social engineering. Training your staff will significantly reduce the risk of a privacy or security breaches.

1 in 4 breaches are a result of social engineering

Recommendations:

- ❑ Develop or update your Privacy Policy (or Retainer) to ensure it reflects the following:
  - What personal information you are collecting (e.g. recordings)
  - How that personal information will be used
  - How long you intend to retain personal information
  - What security safeguards you have in place to secure personal information
  - What jurisdiction personal information will be stored in (e.g. United States) and that laws of that jurisdiction will apply to the personal information
- ❑ Have your client sign a Video Conferencing or Electronic Communication Consent Form acknowledging, amongst other things:
  - The law firm may rely on electronic communication to discuss sensitive information
  - Despite reasonable privacy and security measures, the law firm cannot guarantee personal information will be protected due to evolving online threat landscape
  - The client will implement security measures (e.g. strong passwords) to protect themselves and reduce the risk of a security breach
  - The client will not share a video conference link or password with anyone who is unauthorized to attend
  - The client will not record a video conference session
  - The client will not share documents containing sensitive personal information via video conference platform
- ❑ Develop an internal policy (e.g. Electronic Communication Policy, Video Conferencing Directive) to streamline electronic communication practices and reduce the risk of a privacy and security breach. All staff should use the same video conference platform and default settings.
- ❑ Train staff on: (a) acceptable video conference practices, (b) appropriate settings on the platform, and (c) how to identify privacy or security risks and method of immediately reporting the risks or breaches.

Getting Started.

Conduct due diligence on video conference service providers and implement privacy and security management/accountability within your law firm

Accountability and Oversight

The OPC made references to the importance of developing a privacy culture by setting a tone from the top (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/). Instilling a privacy culture starts with the development of a privacy governance structure. A Privacy Officer or a designated staff must be made accountable for developing, implementing, monitoring and overseeing privacy and security within the law firm and report/escalate concerns to the partner(s).

Recommendations:

- ❑ Ensure a designated individual within your law firm is accountable for overseeing and managing video conferencing, including:
  - Be responsible for or informed of the privacy and security practices of the firm to ensure alignment with the video conference platform
  - Develop video conferencing best practices / policies
  - Stay informed of latest news and releases relating to video conferencing in order to assess and manage evolving risks
  - Stay informed of industry best practices (e.g. caselaw, LawPro, Law Society)
- ❑ Ensure staff are aware of who the designated individual is for video conferencing so they may address questions or concerns with that individual.
- ❑ Delegate to the designated individual the responsibility to assess and/or approve deviation from or exception to the firm privacy and security practices (e.g. using a different video conference platform, removing a default setting).

Fundamentally, in order to be compliant and effective, a privacy-respectful culture needs to be cultivated.

(Office of the Privacy Commissioner of Canada)

Setting Up.

Set appropriate default settings on the video conference platform and develop privacy and security best practices for video conferencing

Initial Steps to Enhance Security

To minimize security breaches, it is necessary to protect the law firm's network to prevent a bad actor from penetrating the network and retrieve your clients' personal information or hold it hostage in exchange for a ransom. The risk of a security breach increases when lawyers work remotely as they may no longer be protected by a secure environment.

Recommendations:

- ❑ Use a virtual private network (VPN) when accessing firm data remotely or logging onto a video conference call remotely.
- ❑ Ensure the VPN is appropriately secured (e.g. use Multi-Factor Authentication).
- ❑ Use Multi-Factor Authentication for all accounts (including video conference platforms) to make them more difficult to access by cybercriminals.
- ❑ If working from home, make sure that your home modems/routers are well secured.
- ❑ Install and keep antivirus and anti malware technologies up-to-date on all devices.
- ❑ When setting up a video conference account, use work email addresses and never a personal account.
- ❑ Use unique and strong passwords to create your account – consider using a password manager (e.g. 1Password to manage your passwords and create strong randomized passwords).
- ❑ Regularly update the video conference application on devices to enhance its security and enable new functionalities which may provide further privacy and security measures.

> ***"…remote workers have become a weak link that threat actors are targeting and that user credentials in offsite computing (home) environments are increasingly at risk…"***
> (ITWorld Canada, March 2020)

Review Permission Settings

The data minimization privacy principle provides that data should only be collected if it is necessary to carry out a service. Law firms should not collect personal information which is not essential to provide a service, such as representing a client. Similarly, if a law firm is to disclose personal information to a Vendor, it should only disclose what is necessary for the Vendor to carry out its services. As such, law firms should review the permission settings on video conference applications to ensure they are not disclosing information which is not necessary for the functionality of the service. For example, while it may be convenient to allow the platform to gain access to your contact list, it may also provide the Vendor more information than is necessary, therefore creating a risk that the Vendor may misuse the data or experience a breach involving your data.

Recommendations:

- ❑ Carefully review permission settings when installing the Platform or when there are updates to the Platform.
- ❑ Consider whether access permissions are necessary (e.g. access to your location, access to your contact list, access to your photos). Be cautious and do not grant access unless necessary.

Setting Up.

Set appropriate default settings on the video conference platform and develop privacy and security best practices for video conferencing

In an effort to reduce (a) video conference hacking (recently known as "Zoombombing"), (b) personal information disclosed to the video conference Vendor, and (c) the risk of disclosing confidential information to other parties on the video conference call, it is necessary to take proactive measures and adjust default settings.

Review and Enable / Disable Default Settings

Recommendations:

- ❑ Depending on the video conference platform, either enable or disable default settings so that it results in the following default functions, which can be adjusted accordingly:
    - All video conferences are private
    - Video conference recording is disabled
    - 'Auto-save' recordings, transcripts, or whiteboard content is disabled to prevent the video conference Vendor from saving the content onto the platform on the cloud
    - Screen-sharing is disabled, other than for the host
    - File transfers are disabled
    - Participants are muted upon entry
    - Participants cannot send private 1:1 messages to each other
    - Make break-out rooms available
    - Guests must wait for the host to join

Sending / Receiving Video Conference Invitation

Recommendations:

- ❑ When scheduling a video conference call, generate a unique password to make the call private and accessible only to invited participants.
- ❑ Send recipients of a video conference invitation the unique conference password in a separate email.
- ❑ If you are a recipient of a video conference invitation, before accepting the invitation, calling into the conference, or clicking on any link, review the email address of the sender and confirm it belongs to the sender so you do not fall prey to a social engineering attack.
- ❑ If you are expecting a large group or individuals whom you do not know, enable registration, which will allow you, as the host, to view the email address of each registrant and compare it to those in attendance on the call.
- ❑ Ensure the title of the video conference does not breach confidentiality or privacy.

Starting a Video Conference.

Set expectations upfront about privacy and security so all parties are informed and can provide meaningful consent

Mind Your Surroundings / Environment

Lawyers have an obligation to take all measures to maintain solicitor-client confidentiality and protect their clients' personal information. Similar to the way lawyers should be mindful of having conversations with their clients in private or removing confidential documents from their desk when they have a visitor, lawyers should maintain that level of confidentiality regardless of their surroundings or environment. A privacy breach or breach of confidentiality can occur when someone overhears or sees information they should not whether by physical or electronic means.

Recommendations:

- ❑ Hardwire the internet connection which will avoid unstable WIFI connection, audio quality and overall attendee experience.
- ❑ Ensure you are in a private and safe location where you may have a confidential conversation without interruption and without others listening in.
- ❑ Turn off your smart devices such as Google Home, Alexa, Siri etc.
- ❑ Minimize background noise or use a headset with a mic to reduce noise.
- ❑ Test the audio and speaker before you begin the video conference.
- ❑ Close documents, windows, browsers on your device which you do not wish for anyone to see (e.g. email / calendar notifications).

In the Waiting Room

Setting a tone about the expectation of privacy and security at the forefront of a video conference will ensure all parties are aligned and any initial issues or concerns can be dealt with upfront.

Recommendations:

- ❑ Develop terms for engaging in the video conference call (e.g. one person speaks at a time, no screen grabbing, no recording, steps to take if you lose connection) and post them in the waiting room so all participants can review them in advance of the video conference call.
- ❑ Mute all participants in the waiting room to avoid discussion amongst parties.
- ❑ Confirm everyone in the waiting room is authorized to be a part of the video conference call and once you have done so admit authorized individuals.

Starting the Discussion

Inform callers whether they can be heard or seen via video so that they do not accidentally disclose confidential information. If you intend to record the video conference call, you must seek explicit consent to do so and reveal the purpose for doing so.

Recommendations:

- ❑ Once you let authorized parties in the video conference call, lock the meeting room to prevent anyone else from joining.
- ❑ Once parties enter a video conference call, inform them whether their sound and/or video is on or off and who controls those features.
- ❑ Confirm the rules of the video conference call.
- ❑ Pursuant to the Law Society's *Rules of Professional Conduct* (Rule 7.2-3), inform other parties to the call whether you will be recording the video conference call and seek explicit consent to do so.

During a Video Conference.

Monitor and maintain privacy and security throughout the video conference call

Maintaining Privacy During the Video Conference

Recommendations:

- ❑ Enable enter / exit chime so that there is notification if someone joins or leaves the video conference.,
- ❑ Be aware of who is entering the call and ensure others on the line are aware of their presence.
- ❑ Be mindful of what might be visible on your video, such as:
    - Documents containing personal or confidential information
    - Other windows/browsers (e.g. email notifications, confidential documents) that are open on your device that may become visible during screen share
- ❑ If the chat feature is enabled, be mindful if your chat is visible to everyone or a particular individual on the video conference call.
- ❑ Mute your mic if you are not talking to avoid revealing information if you talk to someone off the video conference call.

Breakout Room

Recommendations:

- ❑ Before speaking in a breakout room, ensure only intended parties are present.
- ❑ If parties expect confidentiality / privacy in a breakout room, such as in a mediation, the party who enters end exits the breakout room, such as a mediator, should enable the "knock" feature to give warning to those in the breakout room that he/she will be entering. If this feature is not available, the party entering and exiting the breakout room, should provide notice of his/her intention to enter by calling or texting the other party to give warning.

Ending a Video Conference / Post-Video Conference.

Take extra precaution to ensure the video conference ended and securely protect any recordings

Ending a Video Conference Call

Recommendations:

- ❑ Inform the parties to a video conference call of your intention to leave the call if you are leaving earlier than others.
- ❑ Ensure you log out of the video conference call when you leave the video conference.
- ❑ If a party to a video conference call is expected to leave the discussion while others remain on the call, ensure that party has left and is not a silent listener.

Post-Video Conference Call

Law firms should only retain personal information for as long as necessary to fulfill the purpose for which they collected the information for or as prescribed by law. While the Law Society provides guidance to lawyers on retention considerations, law firms should be mindful of non-compliance with PIPEDA and consider what the risk is by retaining video recording, images and a copy of a chat. If a law firm retains information obtained via the video conference call, it will need to implement proportional security measures to protect that information.

Personal information should only be retained for as long as is necessary to achieve the purpose it was originally collected for.

Recommendations:

- ❑ If a conversation, picture or voice recording of a video conference call is to be shared, seek permission to do so from those individuals involved in the call and provide information of the intended purpose for sharing the information.
- ❑ Any recording or copies of images or chats should be saved in the client file, ensuring it is secure and it is accessed only by staff who require access to it. Do not save it in a local folder that does not have proper privacy and security controls.
- ❑ Consider revising your Retention Policy to include video conference recordings and monitor compliance with the retention period.

Breach Preparedness.

Privacy and security is never guaranteed; be proactive and mitigate the harm to both clients and the law firm

Breach Management Plan

Pursuant to PIPEDA, law firms are legally required to notify the OPC when they experience a privacy breach that results in a "real risk of significant harm to an individual". Law firms must keep a record of all privacy incidents and breaches for 24 months. A regulatory investigation or lawsuit for breach of privacy will evaluate the law firm's breach preparedness and ability to minimize the harm once a breach is identified.

> **"Know what personal information you have, where it is, and what you are doing with it. When and where do you collect personal information? Where does that information go? Who can access it, and what do they do with it? You must understand your data before you can protect it!"** – Office of the Privacy Commissioner of Canada, 2019

Recommendations:

❑ Develop or update the firm's Breach Management Plan, which should include the following information:

- What to do if staff identify a breach
- How to respond to a breach, including timelines and owners for each task
- How to contain the breach and retain forensic investigators who are prepared to immediately intervene
- Who to report a breach to, both within the firm and outside the firm (e.g. breach coach, privacy experts), with their up to date contact information
- A process to determine whether the breach should be reported to the Office of the Privacy Commissioner of Canada and how to notify clients affected by the breach
- How to prepare a record of the breach and how long to retain that record

Cyber Insurance

Given the excessive risk of a privacy and security breach, to mitigate the financial harm to the law firm, it is advisable to obtain cyber insurance, which will not only offset costs but take steps to remediate technical and administrative vulnerabilities.

Recommendations:

❑ Obtain cyber insurance to mitigate risk exposure by offsetting remediation costs post-breach such as legal fees, damages, expert fees, technical fees, and other recovery costs.

❑ When purchasing cyber insurance, consider the following:

- Review the difference between a stand-alone policy and an extension to an existing policy
- Review the deductible
- Ensure there is coverage to first and third parties
- Identify whether the policy covers all cyber attacks, non-malicious action by an employee, and social engineering attacks

Well over 28 million Canadians were affected by a data breach in 2019

Video Conference Tools: A Comparison.

The following table provides a comparison of four Video Conference tools: (1) Zoom, (2) Microsoft Teams, (3) Cisco Webex, and (4) Citrix GoTo Meetings. The four selected tools should not suggest that they are the most secure tools on the market, but rather the ones that are the most widely used in the legal industry at the present time.

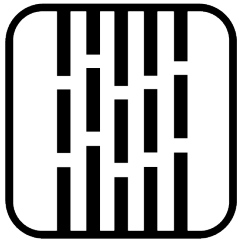
From a security perspective, all four tools comply with multiple industry leading information security standards that are designed to provide an adequate level of security for its customers.

Tools/ Functionality	Zoom	Microsoft Teams	Cisco Webex	Citrix GoTo Meetings
Meeting Room Security	Can secure the meeting room with password. Supports multi-factor authentication for all users. Can lock the meeting room so no one can join once the meeting is started. Has waiting room feature. Supports screenshot watermarking and audio signature.	Does not have password protection for meetings but has settings to control who can join the meeting through lobby settings and structured meetings. Has meeting lobby for attendees waiting. Supports multi-factor authentication for all users.	Can secure the meeting room with password. Can lock the meeting room. Has meeting lobby for attendees waiting.	Can secure the meeting room with password. Can lock the meeting room.
Breakout Rooms	Yes	No	No	No
Meeting Recording	Yes Recording can be stored on cloud or local machine. Cloud recording can be password protected.	Yes Recording is stored in cloud (Microsoft Stream).	Yes Recording is available with paid plans and can be stored on cloud or local machine. Recording can be password protected.	Yes Recording can be stored on cloud or local machine.

Tools/ Functionality	Zoom	Microsoft Teams	Cisco Webex	Citrix GoTo Meetings
Data Residency	Can be stored in Canada. Paid subscribers can opt-in or out of specific data center regions.	Can be stored in Canada.	Can be stored in Canada. Paid plans are required.	Data centers are located in North America. No specific information for data center in Canada.
Video Encryption	Yes	Yes	Yes	Yes
Chat Encryption	Yes	Yes	Yes	Yes
End to End Encryption	No	Yes	Yes	Yes
Meeting Transcript	Yes	Yes	Yes	Yes
Security Certificates	• SOC 2 (Type II) • FedRAMP (Moderate) • GDPR, CCPA, COPPA, FERPA and HIPAA Compliant (with BAA) • TrustArc Certified Privacy Practices • PEU/U.S. and Swiss/U.S. Privacy Shield Certification	• SOC 1 (Type II) • SOC 2 (Type II) • SOC 3 • ISO 27001:2013 • ISO 27017:2015 • ISO 27018 • NIST Cybersecurity Framework • EU GDPR • FedRAMP	• SOC 2 (Type II) • ISO 27001 • Privacy Shield Framework Certified • FedRAMP	• SOC 2 (Type II) • SOC 3 • EU/U.S. and Swiss/U.S. Privacy Shield Certification • TRUSTe Verified Privacy • BSI C5
Screen Sharing	Yes	Yes	Yes	Yes
Chat Setting	Can be disabled. Can be restricted to chat with meeting host only.	Can be disabled.	Can be disabled.	Can be disabled.
File Sharing	Yes	Yes	Yes	No

Glossary

- Audio Watermark – An audio watermark is a unique electronic identifier embedded in an audio signal, typically used to identify ownership of copyright.
- Encryption – Converting information or data into code for the purpose of preventing unauthorized access.
- End-to-End Encryption – A system of communication whereby on those parties communicating can read the messages, preventing third parties from accessing the data while it is in transit from one party to the other.
- FedRAMP - The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- ISO 27001 – Specification for an information security management system of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk management process.
- Multi-Factor Authentication – An authentication method whereby a device user is only granted access after authenticating him/herself twice using multiple credentials.
- Privacy Breach – The misuse of personal information or unauthoritative access to personal information, whether intention or unintentional.
- Privacy Shield – An agreement between the EU and the US allowing for the transfer from the EU to the US. The agreement is designed to create a program for deemed companies to have adequate protection and therefore permitted to transfer information cross-border.
- Security Breach – Unauthorized access to an organization's protected network.
- SOC – An audit which evaluates internal controls, policies and procedures. SOC 1 is a report about internal controls over financial reporting; SOC 2 is a report about security, availability, processing, integrity, confidentiality or privacy controls; and SOC 3 is a publicly available report about security, availability, processing, integrity, confidentiality or privacy controls.
- Social Engineering – A method of manipulating someone to do something, such as reveal personal information, they otherwise would not do.
- Visual Watermark - The Watermark feature superimposes an image, consisting of a portion of a meeting participant's own email address, onto the shared content they are viewing and the video of the person who is sharing their screen.
- Virtual Private Network – A connection between a private network and public network whereby a user can send and receive data in an encrypted manner so that the data remains private even if the connection is intercepted.



BAMBOO

DATA CONSULTING

www.bamboodataconsulting.com