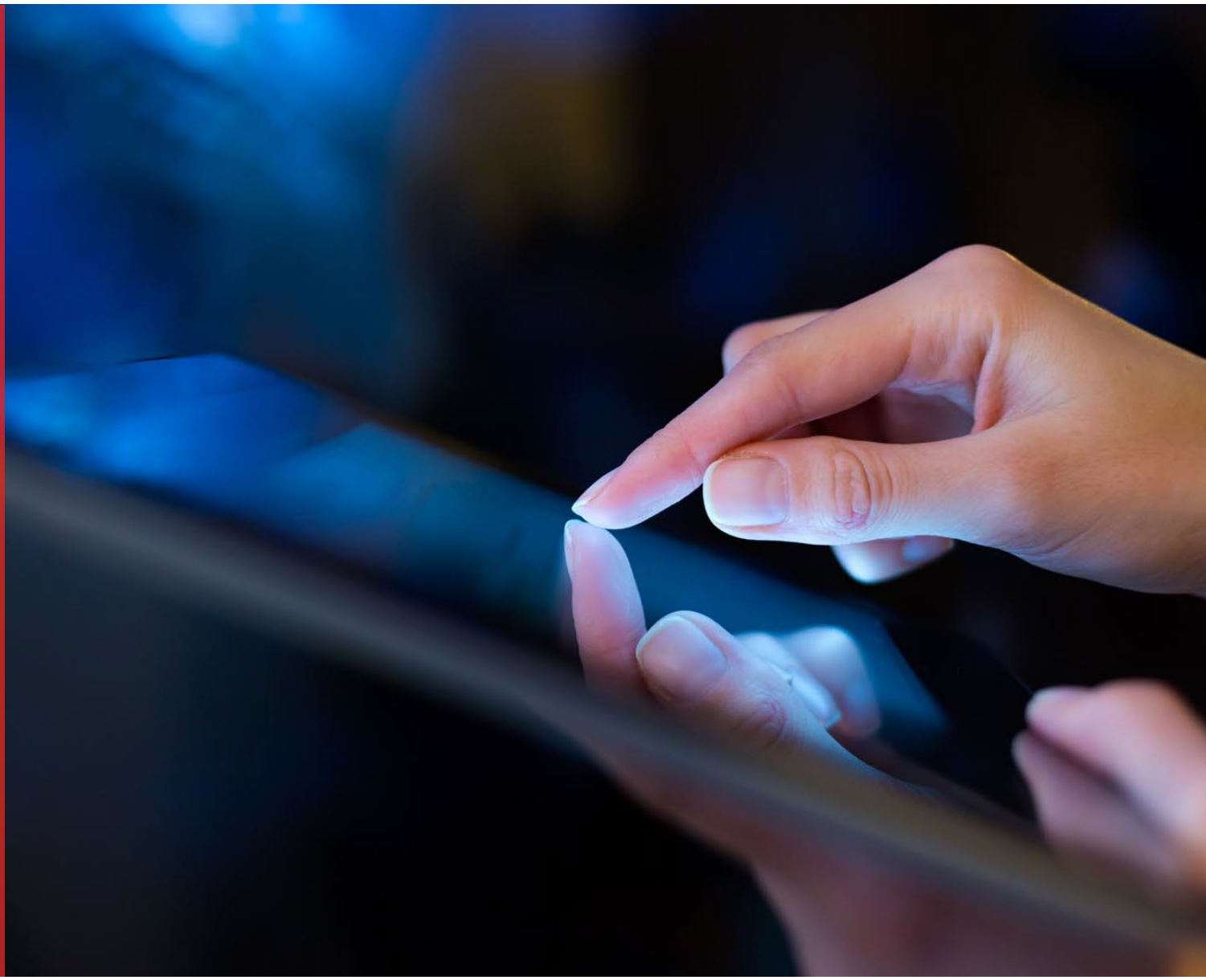
NORTON ROSE FULBRIGHT

Recording and transcribing meetings

Managing risks and maximizing benefits

Norton Rose Fulbright Canada LLP
September 2025



Contents

Introduction	**1**
Legal considerations	**2**
A. Privacy, data security and access to information	2
B. Employment	7
C. Intellectual Property	14
D. Confidentiality	21
E. Regulatory compliance	23
F. Litigation and disputes	25
G. Other legal considerations	29
Governance and best practices	**31**
Appendix A: Internal policy template	**37**

DISCLAIMER

The information provided here is intended solely for general, unbiased informational purposes based on Canadian law as of the date of this paper. It does not constitute legal advice and is not intended to create a solicitor-client relationship. While efforts are made to ensure the accuracy and reliability of the content, its completeness or suitability for a particular situation cannot be guaranteed. There may be changes and developments in Canadian law from the time of its writing that may impact the content.

Introduction

Meeting productivity tools are a standard part of daily workflows, offering features such as recording, transcription, captions, and analytics. Recordings capture audio and video from these meetings, and content shared during meetings. Transcriptions provide written text of spoken dialogue from the meeting. Transcriptions can be automatically generated by AI or machine learning. Captions offer live text of dialogue during meetings. Live translations can also be generated and shared during meetings. These features generate files that can be stored and shared. AI can also analyze the recordings, transcriptions, and meeting content as a corpus of data, and create new content and derivative output based on prompts. The prompts can be user-defined prompts, or pre-populated prompts that can be pre-defined by a company.

These meeting tools enhance productivity, collaboration and accessibility, while raising unique Canadian legal considerations. This paper offers balanced guidance and best practices (including a template internal policy) to maximize the benefits of meeting recordings and transcriptions and mitigate risks.

Legal considerations

A. Privacy, data security and access to information

In Canada, the use of productivity tools to record, transcribe, and summarize meetings raises privacy law and data protection considerations as use of these tools can involve the exchange of personal information, including names, contact details, opinions, and other identifiers. Examples include: (i) privacy obligations for corporations using recording and transcription tools, (ii) security concerns to ensure the information is adequately protected, and (iii) generated documentation that potentially falls within the scope of access to information requests for public-sector organizations.

Applicable privacy laws

Canada has a complex patchwork of federal and provincial privacy laws that may apply depending on the applicable jurisdiction and circumstance in each case:

- The *Personal Information and Protection Electronic Documents Act* (*PIPEDA*)[1] is Canada's federal privacy law applicable to private-sector organizations. *PIPEDA* only applies to employee information of federal works, undertakings or businesses, and does not regulate employee personal information in the private sector.
- British Columbia, Alberta and Quebec have their own private-sector privacy laws that have been deemed substantially similar to *PIPEDA*, with Quebec's *Act respecting the protection of personal information in the private sector* (the *Quebec Private Sector Act*)[2] having been recently amended and imposing additional obligations for organizations processing personal information.
- In the public sector, the *Privacy Act*[3] governs federal organizations, and most provinces have also adopted privacy laws governing personal information collected by public bodies at the provincial level.
- In the healthcare sector, a majority of provinces have legislation in force governing the collection, use, disclosure and storage of personal health information (see *Section E – Regulatory Compliance* for more information on this topic).
- There can be industry-specific laws, regulations and guidelines that also govern how personal information should be handled by organizations (e.g., organizations in the financial sector can be subject to additional guidance from provincial regulators; see *Section E – Regulatory Compliance* for more information on this topic).

Broadly, these laws govern the collection, use and disclosure of personal information by organizations, as well as individuals' rights of access and correction to their personal information and, in the case of public-sector laws, the right to request information from organizations. One or more privacy laws may apply depending on the meeting context, the nature of an organization (i.e., private or public sector), its activities and the province of residence of individuals about

---

[1] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
[2] *Act respecting the protection of personal information in the private sector*, CQLR, c P-39.1.
[3] *Privacy Act*, RSC 1985, c P-21.

whom personal information is collected, used or disclosed (who are either participating in a meeting or whose personal information is discussed during the meeting).

Personal information and privacy considerations

Personal information is generally defined as any information capable of identifying an individual, either when used alone or in combination with other information. Depending on the context, audio or video recordings and transcripts of meetings can contain information that is considered personal information under privacy laws in Canada, giving rise to various data protection obligations and rights for the individuals about whom this information is collected. This personal information can be about individuals participating in a meeting, or about individuals whose personal information is discussed in the meeting.

Under Canadian privacy laws, organizations must ensure personal information is collected, used, and disclosed in a manner that is lawful, transparent, and limited to specific, legitimate purposes. This includes implementing appropriate safeguards to protect the confidentiality and integrity of the data throughout its lifecycle (see “Data Security” section below for more information). In Quebec, organizations are explicitly required to establish and implement governance policies and practices protecting personal information throughout its lifecycle and make this information available to the individuals about whom personal information is collected.[4]

Consent and transparency

Consent and transparency are foundational principles in Canadian privacy law. Participants in a meeting ought to be made aware at the outset of the meeting that the session will be recorded and the recording may be processed by tools using AI or machine-learning. This notification can be provided at the time of collection and/or supported by a more comprehensive privacy policy that clearly explains what data is being collected, how it will be used, with whom it may be shared, how long it will be retained, and what rights individuals have over their personal information.

If sensitive personal information is involved, or if the collection or use of the personal information would otherwise not be reasonably expected by the individuals, an express consent from individuals may be required. This consent must be freely given, specific, informed, and unambiguous. As a best practice, meetings that involve sensitive information about one or more of the participants and where the productivity tools are not essential to the purpose of the meeting (e.g., a meeting discussing the health condition of an employee with human resources) the clear consent of the relevant participants should be obtained.

A particularly sensitive category of personal information is biometric data, which includes voiceprints and facial recognition features. When AI tools analyze audio or video recordings to identify speakers or enhance transcription accuracy, they may be processing biometric information. This type of data is subject to stricter legal requirements due to its potential for misuse and its unique link to a specific individual. Under certain privacy laws, organizations may be required to obtain the express consent of the individual before collecting or using biometric data. In addition, under *the Quebec Private Sector Act*, organizations must also notify the privacy regulator ahead of deploying systems using biometric data to identify or authenticate individuals.

[4] Section 3.2 of the *Quebec Private Sector Act*.

Clear and limited purposes

The purposes for which productivity tools process meeting data should be clearly defined and limited to what is necessary. Common purposes include transcription for accessibility, summarization for efficiency, and compliance monitoring. If the data is to be used for secondary purposes, such as training AI models or improving algorithms, organizations should make these secondary purposes clear to individuals, and additional consent requirements may be required for these secondary purposes. Using personal information beyond its original purpose without proper authorization can lead to the imposition of regulatory penalties and may result in reputational harm.

Disclosure of personal information

Disclosure of personal information collected through the recording, transcription or summary of a meeting should also be reasonable and proportionate. Organizations should consider who should have access to recordings, transcripts, summaries. If these files are to be widely circulated (or posted on an internal platform where everyone can access them), this should be conveyed to all meeting participants.

As mentioned earlier, the *Quebec Private Sector Act* includes some of the most stringent privacy requirements in Canada. One of its key provisions requires organizations to conduct a privacy impact assessment (PIA) prior to implementing any project to acquire, develop, or overhaul an information system that involves the collection, use, communication, keeping, or destruction of personal information, or when the personal information is transferred outside of Quebec. A PIA must evaluate the potential privacy risks, outline mitigation strategies, and ensure the project complies with the law. Depending on the tools implemented and where the data is processed, recording and transcription tools for meetings may trigger this PIA requirement.

Rights of individuals

Individuals have robust rights under Canadian privacy laws. These include the right to access their personal information, the right to request corrections to ensure accuracy, and the right to withdraw consent at any time, subject to legal or contractual obligations. Recordings, transcripts or summaries of meetings, to the extent they contain personal information about individuals, could fall within the scope of such requests.

The *Quebec Private Sector Act* also grants individuals the right to be informed about the use of automated decision-making where no human review occurs, including the logic behind such systems and the potential consequences for the individual. This right is designed to empower individuals and promote accountability in the use of AI technologies. If personal information is used for automated decision-making, such as using AI-generated meeting transcripts to assess employee performance, this use should be considered separately. It is recommended that such processing be avoided unless it is strictly necessary and appropriately disclosed to the concerned individuals. This approach helps to mitigate against compliance risk from a privacy law standpoint.

Public sector and access to information

Freedom of information access requirements under applicable privacy laws grant the public the right to access records under the control of a public body. These records include those created or stored using productivity tools. When these tools are used in meetings, such as for recording, transcribing, or summarizing discussions, any resulting records may be subject to access requests, depending on their content and purpose.

For example, in British Columbia, if a meeting is transcribed or recorded, the record of the meeting may be subject to the privacy and access rules under the BC *Freedom of Information*

and Protection of Privacy Act (the *FOIPPA*).[5] Records in this form, including those that are generated with AI, need to be managed in the same way as any other notes of the meeting and may be subject to freedom of information requests.

In Alberta, the *Freedom of Information and Protection of Privacy Act* (the Alberta *FOIP*)[6] and the *Health Information Act* (the Alberta *HIA*)[7] may apply to recordings of meetings. The Alberta *FOIP* and the Alberta *HIA*[8] provide that, whenever a public body collects personal or health information, notice must be provided that includes:

1. The legal authority for the collection.
2. How it will be used.
3. The information position title, business phone number and business mailing address of an employee or affiliate who can answer questions about the collection.

Such recordings may also be subject to access requests under the Alberta *FOIP* or *HIA.* If the meeting involves a public body (*e.g.,* a university), the file of the recording will be a record subject to the Alberta *FOIP*, meaning that any individual can make an access request for that record, and the public body may have to provide it to the applicant. For meetings involving personal health information, participants would have similar access rights to their own health information under the Alberta HIA, including recordings of meetings that discussed personal health information.

In Saskatchewan, the *Freedom of Information and Protection of Privacy Act* (the Saskatchewan *FOIP*)[9], *The Local Authority Freedom of Information and Protection of Privacy Act* (the Saskatchewan *LA FOIP*),[10] *The Health Information Protection Act* (the Saskatchewan *HIPA*)[11] and *The Archives and Public Records Management Act*[12] may be relevant for recordings of meetings.

The Office of the Information and Privacy Commissioner of Saskatchewan has released advisories[13] that confirm a recording of a meeting is a record, and if the meeting involves participants from public bodies, then it must be decided whether the recording is an official record or transitory record under *The Archives and Public Records Management Act*. Whether the recording is an official record or transitory record will guide organizers in deciding how to arrange for storage and preservation in their electronic filing systems or when the record should be destroyed. If any access request under the Saskatchewan *FOIP*, the Saskatchewan *LA FOIP* or the Saskatchewan *HIPA* is received and the recording of the meeting exists, at that time, the record may have to be disclosed under the Saskatchewan *FOIP*, the Saskatchewan LA FOIP or the Saskatchewan HIPA (subject to appropriate exemptions).

---

[5] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 ("BC *FOIPPA*").
[6] *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25 ("Alberta *FOIP*").
[7] *Health Information Act*, RSA 2000, c H-5 ("Alberta *HIA*").
[8] ss.34(2) of the Alberta *FOIP* and ss. 22(3) of the Alberta *HIA*.
[9] *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01 ("Saskatchewan *FOIP*").
[10] *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1 ("Saskatchewan *LA FOIP*").
[11] *The Health Information Protection Act*, SS 1999, c H-0.021 ("Saskatchewan *HIPA*").
[12] *The Archives and Public Records Management Act*, SS 2015, c A-26.11.
[13] Office of the Information and Privacy Commissioner of Saskatchewan, "Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on Pandemic and Virtual Meetings," April 2020: <https://oipc.sk.ca/advisory-from-the-office-of-the-information-and-privacy-commissioner-of-saskatchewan-on-pandemic-and-virtual-meetings/>.

Transparency is a key principle. Public bodies must be able to account for how information is collected, processed, and stored using these tools. This includes maintaining clear documentation of how recording and transcription tools are configured, what data is retained, and how it can be accessed or disclosed in response to an information request. If productivity tools are used to generate summaries or automate note taking, the outputs may also be considered records, especially if they inform decision-making or are shared internally.

Organizations should ensure that records created during meetings are properly managed and classified. This includes determining whether meeting recordings, transcripts, or summaries constitute official records that must be retained and made accessible under applicable law. If so, they must be stored in a manner that ensures their integrity, retrievability, and security.

To support this determination, organizations can consider the nature and function of each type of meeting output. Recordings typically include audio, video, and any content shared on screen during the meeting. These may qualify as official records depending on the topics addressed in the meeting. Transcripts, which are generated by systems that convert spoken dialogue into text, can assist with documentation and accessibility but may not be considered authoritative unless reviewed and validated. AI-generated summaries, which are created by analyzing meeting content through prompts or automated processes, are generally not treated as official records unless they are relied upon for compliance, audit, or legal purposes. Organizations should evaluate whether each type of output reflects substantive content that must be preserved, and apply appropriate governance measures to ensure accuracy, security, and compliance.

Data retention

Data retention is another critical consideration, as organizations must define and document how long they will retain both the original recordings as well as any derivative products, such as transcripts or summaries. Retention periods should be limited to what is necessary for the stated purposes, after which the data should be securely deleted or anonymized. As detailed above and elsewhere herein, documentation and data generated from productivity tools may contain personal information, confidential information or otherwise commercially sensitive information. Implementing a retention policy and ensuring that data is destroyed as required in accordance with such policy further mitigates the organization’s risk that such data becomes the subject of a confidentiality incident.

Organizations should make an informed assessment as to whether meeting recordings and transcripts should be treated as a distinct data category, and if so, whether to implement a formal retention policy governing the lifecycle of information generated by these tools. Proper implementation of such policies reduces the risk of confidentiality incidents and supports compliance with applicable data protection frameworks. To this end, recording and transcription tools can offer features that allow organizations to manage retention settings, including defining how long data is kept, when it should be deleted, and how it should be disposed of.

Data security

Organizations using productivity tools for meetings must implement robust safeguards to protect personal information. These technical safeguards may include encryption, access controls, secure storage, and regular audits to ensure compliance with applicable privacy laws. Administrative measures such as staff training, privacy policies, and incident response plans are equally important to ensure data is handled responsibly throughout its lifecycle. Often security policies of Canadian federal and provincial public bodies will require appropriate security safeguards as to how and where such recordings are to be stored, including, but not limited to,

encryption, proper access controls, appropriate physical security for devices, network security and antivirus software.

Since service providers offering productivity tools or cloud services may be located or otherwise hosted outside of Canada, data residency should also be taken into consideration when deploying such tools or services. In Canada, organizations must assess whether personal information will be transferred across borders and, if so, must ensure that equivalent levels of protection are maintained. Under *PIPEDA* and other private sector privacy laws, organizations are required to inform individuals if their data will be stored or processed in another country, and what risks may be associated with such transfers. The *Quebec Private Sector Act* imposes the requirement to conduct a PIA before transferring data outside Quebec and ensuring the foreign jurisdiction offers adequate protection. Public sector organizations may also be subject to further limitations regarding the transfer of personal information outside of Canada.

When using third-party service providers, organizations remain accountable for the personal information processed on their behalf. This means they must conduct due diligence, enter into binding agreements that specify privacy and security obligations, and monitor compliance with these requirements. Service providers should be contractually obligated to use the data only for authorized purposes, to implement appropriate safeguards, to notify organizations of any breach of the information they are handling on their behalf, and to destroy the information after the end of the agreement.

Segregation of data is essential to prevent unauthorized access or data leakage between clients or systems. When considering various tools, organizations should ensure their own set of data is logically or physically isolated or separated from that of other organizations, especially when using shared infrastructure or multi-tenant cloud environments. This approach helps to maintain confidentiality and integrity, particularly when sensitive or regulated data is involved.

Finally, organizations must prepare for cybersecurity incidents by implementing proactive risk mitigation strategies. One such strategy is to minimize the storage of sensitive data, such as video or audio recordings, by deleting them as soon as they are no longer needed and retaining only the necessary transcripts or summaries. This reduces the potential impact of a confidentiality incident. Many privacy laws in Canada require organizations to report certain breaches to regulators and affected individuals and maintain a record of all confidentiality incidents.

B. Employment

Collection, use, and disclosure of employee personal information

Where an employee is a participant in a workplace meeting that is recorded or transcribed (including with virtual meeting software), employee personal information will likely be collected as a result. Depending on the scope of the applicable privacy law, this personal information will be subject to the requirements discussed in *Section A - Privacy, Data Security and Access to Information.* A work-related meeting also involves employment law considerations.

As an example, the BC *Personal Information and Protection Act* (the BC *PIPA*)[14] generally requires provincially regulated private sector organizations to limit collection of personal information to only purposes that a reasonable person would consider appropriate in the

[14] *Personal Information and Protection Act*, SBC 2003, c 63 ("BC *PIPA*").

circumstances.[15] While consent is not required if the collection, use, or disclosure of employee personal information is reasonable for the purposes of establishing, managing, or terminating an employment relationship between the employer and the individual,[16] employers must still generally provide advance notice of collection, use, and disclosure of employee personal information and the purposes for such collection.[17]

That said, neither consent nor notification is required if the BC *PIPA* expressly permits the collection, use, or disclosure of personal information without consent under sections 12, 15, and 18 respectively.[18] Some non-exhaustive examples of situations where consent is not required include:

- Where it is reasonable to expect that collection, use, or disclosure with consent would compromise the availability or accuracy of the personal information and the collection, use, or disclosure is reasonable for the investigation or proceeding.[19]
- Where collection, use, or disclosure is necessary to determine the individual's suitability to receive an honour, award or similar benefit.[20]
- Where collection, use, or disclosure is required or authorized by law.[21]

Privacy regulators in Canada have issued guidance on the broader issue of employee monitoring in the workplace, which highlights the need to balance such monitoring with the employees' right to privacy and cautions against over-collection of employee personal information.[22] Such guidance emphasizes that while monitoring may be considered reasonable or even necessary in certain circumstances – for example, where necessary for safety, for asset protection, or to ensure compliance with policies – any such monitoring must be limited to what is minimally necessary in order to fulfill the purposes for such monitoring. These considerations apply equally in an organization's use of recording and transcription tools, including such functions in virtual meeting software. Privacy regulators have also, more generally, published guidelines to help private sector businesses comply with legislative requirements, with regard to the management, collection, use, retention, destruction, and disclosure of personal information,[23] which can include collection of such information through recordings and transcription.

Questions that an employer should ask itself prior to recording or transcribing a meeting in which an employee is a participant include whether:

- Consent and/or notice is required for the recording or transcription, and if so whether that consent has been obtained and/or that notice has been provided. While arguable exceptions to consent and notification may exist in specific circumstances, if recording a meeting with an employee, employers should generally notify the employee of the

---

[15] ss. 11, 14, 17, BC PIPA.
[16] ss. 13(2)(b), 16(2)(b), 19(2)(b), BC PIPA.
[17] ss. 13(3), 16, 19, BC *PIPA*.
[18] ss. 13(4), 16(4), 19(4), BC *PIPA*.
[19] ss. 12(1)(c), 15(1)(c), 18(1)(c), BC *PIPA*.
[20] ss. 12(1)(f)(i), 15(1)(f)(i), 18(1)(f)(i), BC *PIPA*.
[21] ss. 12(1)(h), 15(1)(h), 18(1)(o), BC *PIPA*.
[22] BC Office of the Information & Privacy Commissioner, "Employee Privacy Rights Guidance Documents," November 2017: <https://www.oipc.bc.ca/documents/guidance-documents/1995>; Office of the Privacy Commissioner of Canada, "Privacy in the Workplace: May 29, 2023": <https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/>.
[23] Commission d'accès à l'information, "Protéger les renseignements personnels: capsules vidéo>," <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/capsules-video; BC Office of the Information & Privacy Commissioner, "A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations," October 2015: <https://www.oipc.bc.ca/documents/guidance-documents/1371>.

recording, what the recording will be used for, and who the employee may contact with any questions.

- The recording or transcription is being done for a reasonable purpose.
- The recording or transcription is limited to only what is necessary to fulfill that reasonable purpose and only used and disclosed in relation to that purpose. For instance, is it necessary to record both the visual and audio from the meeting? Is it necessary to keep a record of the written messages in the meeting, including any side conversations that may be occurring in the meeting?
- There is a less privacy-invasive alternative to effectively achieve the purposes that the recording and transcription are intended to achieve.
- The recordings and transcriptions are being stored securely such that access is limited to only the individuals who require such access for the purposes identified for the recording or transcription, maintained only for as long as necessary or legally required, and deleted thereafter.
- The degree of sensitivity of the personal information in the recording or transcription may attract a higher expectation of privacy and therefore merit more stringent security measures with respect to retention.

Employees may wish to use recording or transcription tools for meetings with entities external to the employer (for instance, clients or other businesses). In such cases, it is prudent for employers to direct these employees to consider, and consult a designated contact within the organization as needed, whether the considerations above have been taken into account for any personal information that may be captured, including whether different or additional issues may need to be factored in if that external entity is located in another jurisdiction.

Depending on the jurisdiction(s) in which they operate, an employer may also be required by statute to develop and implement a privacy policy generally, or an electronic monitoring policy specifically. For instance, provincially regulated employers in Ontario with 25 or more employees are required by the Ontario *Employment Standards Act, 2000*[24] to have a written policy on electronic monitoring of employees, setting out whether or not the employee electronically monitors employees, and if so, details of how and in what circumstances that monitoring occurs and the purposes for which the information collected may be used.[25]

Although such a policy will not completely remove an employee's expectation of privacy in the workplace, particularly where some personal use of the employer's information technology systems is permitted or reasonably expected,[26] nor will it remove an employer's obligation to account for any applicable legislative requirements, a clear and unambiguous policy can diminish expectations of privacy on work equipment or systems. As such, even if not expressly required by statute, employers may wish to consider implementing a robust privacy policy that addresses expectations and obligations for the collection, use, and disclosure of personal information, including but not limited to personal information obtained through the recording and transcription of meetings.

---

[24] *Employment Standards Act, 2000*, SO 2000, c 41.
[25] Part XI.1, *Employment Standards Act*.
[26] See for instance *R. v. Cole*, 2012 SCC 53, in which a majority of the Supreme Court of Canada concluded that Canadians may reasonably expect privacy in personal information contained on computers, whether found in the workplace or at home, where personal use is permitted or reasonably expected, and that while workplace policies may diminish such expectation of privacy in a work computer, the expectation will not be entirely removed.

For unionized workplaces, there may be additional relevant requirements under collective agreements to consider. Further, the heightened scrutiny by unions of workplace policies that could infringe on employee privacy should be taken into account.

Third-party recordings

It is best practice for employers to instruct employees participating in a meeting with third parties in the course of their employment to be aware of any recordings or transcriptions that the third party may make of that meeting and, if so, to:

- Obtain further information from the recording/transcribing party about the purposes and intended uses of that recording or transcription, which may include requesting a copy of any relevant privacy policy if the recording or transcribing entity is not a natural person.
- Be mindful of whether issues concerning sensitive information that may be shared in that meeting (which may include personal information of not only the employee but of others, as well as confidential or proprietary information) could be engaged as a result of such recording or transcription.
- Consider whether the circumstances are such that requesting a copy of the recording or transcript would be prudent to ensure accuracy or alignment on the matters discussed at the meeting (for instance, if discussing terms of a potential services agreement or the sale or purchase of a product).

Whether or not a recording or transcription is taking place, it is inadvisable for an employer to permit or condone employees acting in their capacity as its representative to act outside of the scope of their work responsibilities. However, the growing possibility of meetings (and other interactions) being documented via the use of such tools further underscores the importance of employers communicating, clearly and explicitly, to employees the expectation that while they are performing their duties or representing their employers, whether at the workplace or at a work-related event or meeting, they are to comply with their employer's policies and to conduct themselves within the proper scope of their authority and duties at all times.

Surreptitious recordings of workplace meetings

While Canada's *Criminal Code* provides that it is illegal for an individual to wilfully intercept (including recording the substance, meaning or purport of[27]) a private communication that was not intended to include that individual as a participant,[28] such prohibition would not restrict individuals from surreptitiously recording workplace conversations where they are intended to be a recipient of the conversation and in which they are participating in their capacity as an employee (as opposed to acting as a representative of the employer, like a manager). Organizations must contend with the distinct possibility that employees may create surreptitious recordings of workplace meetings, particularly as more and more meetings are held virtually. The existence and content of surreptitious recordings of workplace conversations made by an employee has been considered and utilized by Canadian courts deciding employment-related claims, with different results.

There may be circumstances in which surreptitious recording behaviour supports the termination of the employee's employment for just cause. *In Shalagin v. Mercer Celgar Limited Partnership* [*Shalagin*],[29] an employee had his employment terminated without cause by his employer and subsequently brought several legal proceedings against the employer in relation to said

---

[27] s.183, *Criminal Code* of Canada.
[28] s.184, *Criminal Code* of Canada.
[29] *Shalagin v. Mercer Celgar Limited Partnership*, 2023 BCCA 373 ["*Shalagin*"].

termination, including a wrongful dismissal civil claim. During document disclosure in the proceedings, the employee disclosed many workplace conversations he had surreptitiously recorded during his multi-year employment relationship (including one-on-one meetings; over 100 “toolbox talk” meetings; at least 30 meetings with supervisors and HR; and conversations among co-workers occurring ambiently in the workplace).

It was not disputed by the employee that he was bound by the employer’s policies, including a Code of Business Conduct and Ethics that required him to, among other things, conduct himself in an honest and ethical manner when dealing with other employees. The employee testified that he had created these recordings for the initial purpose of improving his English, but then subsequently for the purpose of hoping to create a record of interactions with management personnel in which they made a discriminatory or bullying remark in relation to which he could file a complaint. Upon learning of the recordings, the employer successfully argued in the civil proceeding before the British Columbia Supreme Court that it had after-acquired just cause for termination as a result. The employee appealed the trial decision to the British Columbia Court of Appeal, which dismissed the appeal and upheld the finding of just cause.

While the British Columbia Court of Appeal declined to equate the employee’s surreptitious recordings to dishonesty, it noted nonetheless that the recordings were underhanded and would be regarded by most employers as misconduct going to the heart of the employment relationship, and that they violated the privacy of not only those who were recorded but also that of the individuals who were discussed in the recordings. The British Columbia Court of Appeal noted the trial judge’s observations that the employee had acted unethically in surreptitiously recording individuals, as he knew they would be uncomfortable if they knew of the recordings, and that there was a public policy concern with condoning the employee’s actions as it would encourage other employees who felt mistreated to routinely make secret recordings of co-workers in violation of those coworkers’ individual privacy rights.

Surreptitious workplace recordings, including using virtual meeting software, can similarly justify discipline in the unionized context as well, potentially up to and including termination of employment depending on the individual circumstances.

For instance, in *Ontario Public Employees’ Union, Local 125 v Lambton College of Applied Arts and Technology*,[30] an employee grieved the termination of his employment for just cause on the basis that, among other things, he had made three surreptitious video recordings of meetings with his employer to discuss that complaint, without the consent of those involved in the meetings and using software that did not indicate to the participants that recording was occurring. The employer had a policy on recording requiring that all members to a conversation be informed of and provide explicit consent to the recording. The arbitrator concluded that the employee had behaved dishonestly and disrespectfully towards the other participants in the meetings, and that in the circumstances, the surreptitious video recording was a serious breach of trust and the discipline was appropriate. However, given the mitigating factors in the circumstances, including the grievor’s lengthy service and clear disciplinary record, the arbitrator found that discharge was excessive in these circumstances and substituted the termination for an unpaid one-week suspension.

In Quebec, arbitral case law establishes that secretly recording someone does not need to be specifically prohibited by an employer in order to constitute a breach of the employee’s duty of

[30] *Ontario Public Employees’ Union, Local 125 v Lambton College of Applied Arts and Technology*, 2023 CanLII 60382 (ONLA).

loyalty. The frequency of clandestine recordings and the period during which the employee makes them can, depending on each individual set of circumstances, constitute either a mitigating or aggravating factor in assessing the proportionality of the sanction imposed by the employer. A single isolated act will warrant a less severe disciplinary measure, whereas repeated acts will justify a more severe disciplinary sanction.

For instance, *in Syndicat des travailleurs de Demix (Longueuil et LaSalle)-CSN c Demix Béton, une division de Holcim (Canada) inc. Établissements de Longueuil et LaSalle*,[31] the employee admitted to having recorded meetings of the grievance committee and the joint occupational health and safety

committee, as well as conversations, discussions, and meetings in the context of investigations he was conducting. He also recorded conversations in the workplace whenever the employer was present or when the employee himself was involved, either personally or as a union representative. He claimed he did not record his colleagues. These recordings were made without the knowledge of the individuals concerned.

The employee was dismissed for breaching his duty of loyalty or confidentiality by secretly recording the conversations of those involved, thereby breaking the bond of trust. The adjudicator in this case noted that the misconduct alleged — namely, recording conversations without the knowledge of those being recorded — constituted a serious breach of the duty of loyalty, and that clandestine recordings could not be tolerated in the workplace, regardless of the reasons for resorting to such means, referring to the employee's duty of loyalty under article 2088 of the *CCQ* (which requires the employee to be honest with the employer, and is premised on the notion that an employer must be able to trust the employee, whether at the workplace or elsewhere). The dismissal was found to be justified.

In *BC Society for the Prevention of Cruelty to Animals v Canadian Union of Public Employees, Local 1622*,[32] a union grieved the termination of an employee's employment for just cause on the basis that, among other things, the employee had surreptitiously recorded the employer's private discussions in which he was not a participant. Specifically, the employee surreptitiously recorded an investigation meeting with the employer in which he was a participant, and at one point he left the room for the employer's management team to conduct a private meeting but left his phone on the table, which then recorded the employer's private conversation.

The employee subsequently listened to and quoted from the recording of the employer's private discussions in a social media post. The arbitrator noted that the making of a recording, at work, without the consent of the other parties in attendance, was conduct meriting discipline,[33] and the seriousness of the employee's misconduct was further exacerbated by the fact he had recorded a conversation to which he was not a party. In this case, the recording of the employer's private conversations alone was deemed serious enough on its own to justify dismissal.[34]

---

[31] *Syndicat des travailleurs de Demix (Longueuil et LaSalle)-CSN c Demix Béton, une division de Holcim (Canada) inc. Établissements de Longueuil et LaSalle*, 2016 CanLII 64960 (QC SAT); See also: *Fraternité des constables spéciaux d'Hydro-Québec, section locale 4785 (SCFPFTQ) et Hydro-Québec,* 2016 QCTA 500; *Rabbath* et *Société des casinos du Québec inc. (Casino de Montréal)* D.T.E. 2013T-489.
[32] *BC Society for the Prevention of Cruelty to Animals v Canadian Union of Public Employees, Local 1622*, 2025 CanLII 5358 (BCLA) [*"BCSPCA"*].
[33] *BCSPCA* at para 216, citing to *Terrapure Environmental v. International Union of Painters and Allied Trades, District Council 138 (Jeremy Arnot Termination),* 2021 CanLII 72624 (Love) at paras. 243 and 245.
[34] *BCSPCA* at para 219.

On the other hand, there may be circumstances in which an employee could be found to be justified in making a secret recording of a workplace conversation. In *Rooney v GSL Chevrolet Cadillac Ltd* [*Rooney*],[35] an employee resigned from his employment, claiming his employer had constructively dismissed him for disagreements with certain workplace changes. He sought to introduce into evidence audio recordings he had surreptitiously made of meetings with his supervisors. The employer, in turn, applied at the start of the trial to amend its pleadings to assert after-acquired just cause to terminate the employee's employment, on the basis that by recording his supervisors without their knowledge or consent, the employee had breached the terms of his employment. The employer also objected to the admissibility of the recordings on the basis that, among other things, their admission was contrary to public policy as the surreptitious recordings undermined the employment relationship.

The Alberta Court of King's Bench denied the employer's request to amend its pleadings to allege after-acquired cause as the request had not been made in a timely manner and the course of litigation up to trial had not involved an allegation of just cause. (On this issue, a different outcome may have been reached had the employer sought to amend its pleadings at an earlier stage in the process.) The Alberta Court of King's Bench also rejected the employer's public policy argument in objecting to the records' admissibility, observing that an individual in a conversation could record that conversation without the consent of the other participants in the conversation. While it acknowledged that surreptitious recordings of workplace conversations could cause irreparable damage to the employment relationship, the Alberta Court of King's Bench noted there was support in Canadian case law for the proposition that in certain circumstances, such recordings could be warranted. Identified examples of such circumstances included use of a recording by an employee to address a power imbalance with the employer and to objectively establish their credibility where such credibility was being challenged by the employer, or situations where the employment relationship had already broken down (as was the case here).

Despite refusing the employer's request to amend its pleadings to assert after-acquired cause, the Alberta Court of King's Bench nonetheless considered the underlying trial decision in *Shalagin*. It distinguished the trial decision in *Shalagin* from the circumstances before it on the basis that (a) the employer in *Shalagin* had relied on written policies that the employee acknowledged bound him, whereas the employer in *Rooney* had not adduced any evidence of policies signed by the employee relating to recording conversations with fellow employees, and (b) the employment relationship in *Rooney* was already frayed at the time of the first recording due to the employer engaging in conduct amounting to constructive dismissal, which in turn justified the employee recording workplace conversations to address the power imbalance in the employment relationship. The Alberta Court of King's Bench concluded that even if it had permitted the employer's request to amend its pleadings to assert just cause for termination, it would have dismissed such argument.

Ultimately, the case law on surreptitious recordings in the workplace is still developing, and to date there is a spectrum of potential outcomes in terms of how such recordings may be used in subsequent employment-related legal proceedings. Organizations confronted with recordings or transcriptions of workplace meetings made by a dismissed employee will need to consider that those recordings may be put to use by both parties and for very different purposes, depending on the facts.

---

[35] *Rooney v GSL Chevrolet Cadillac Ltd*, 2022 ABKB 813 ["*Rooney*"].

In any case and as noted above, a clear and consistently enforced policy addressing the recording of meetings and the use of recording/transcription functions in virtual meeting software (including but not limited to restrictions on use of such functions and the resulting records and consent and notification requirements) and reasonable efforts to make employees aware of, and train them on, said policy, can make a meaningful difference in how surreptitious recordings are viewed by a decision-maker.

Benefits in the employment context

While care must be taken to ensure that privacy and other considerations engaged by recording and transcription tools (e.g., disclosure of proprietary information, inappropriate use of recorded content) are accounted for, there are many benefits that these tools can and do offer to employers and businesses generally – including the following:

- Recordings and transcripts serve as contemporaneous documentation of a meeting should there be a need to consult an objective record subsequently (for instance, to resolve a conflict or even serve as evidence for whether or not something was said by a participant), or to rely on a record for purposes of managing an employment relationship (for instance, investigating a report of conduct in breach of an employer's policy during a meeting).
- These meeting tools allow organizations to better accommodate participants who may not otherwise be able to fully access or participate in a meeting, including as a result of a protected characteristic under human rights law (for instance, transcription can support an employee who has hearing loss or may not physically be able to take notes).
- In an increasingly remote working world, the recording or transcription of a meeting can also come in handy where team members are spread across various time zones – particularly where logistical challenges in coordinating meetings may arise due to rights to disconnect from work outside of regular working hours.

C. Intellectual Property

For intellectual property law, in the context of meetings, it is important to distinguish between the recording and transcript themselves, and other works that may be presented or shared during the meeting and captured by the recording and transcript.

Recordings and transcripts of virtual meetings may be protected as copyrighted works. Further, the content of recordings and transcripts may contain works (e.g., speeches, presentations, or other original works) that are separately protected by copyright. Sharing or reproducing copyright works without permission may infringe the rights of the owner or may be considered an exception depending on the meeting context. Additionally, other forms of intellectual property may be disclosed during meetings, including patentable inventions or designs, necessitating further consideration.

Copyright

The copyright owner has the exclusive right to reproduce, distribute, perform, or communicate the work to the public. Sharing or reproducing the copyrighted work without permission may infringe the rights of the owner. Any copyright in the recording does not automatically grant the right to use or reproduce any underlying works that may be captured in the recording. Before sharing and copying a recording and transcript, it is important to identify copyright work captured by the recording and transcript and confirm whether additional permission to share the work is required from the copyright owner.

Recording

A recording of a virtual meeting records the spoken words of participants (and other sounds made during the meeting) to generate and output an audio recording file. The recording of the virtual meeting may also record video images of the participants during the meeting to generate and output an audio/visual recording.

The recording can involve different copyright works and protected rights.

In Canada, copyright protects original works of authorship that involve human skill and judgment.[36] The recording itself may be considered a copyright work if it is an original work involving human skill and judgment.

The recording may embody content such as underlying literary or musical works. For example, a participant can read out a poem (e.g., original text) that is protected as a literary work. As another example, if a song is played or uttered during the meeting it may be protected as a musical work.

A meeting may also involve content shared by participants during the meeting. For example, there may be a file upload tool or a chat feature that allows participants to drag and drop files into a group chat for access by the other participants. The shared content may include files, images, documents, or presentations that are protected by copyright. The recording may capture and record the shared materials.

A video (e.g., audio/visual) recording of the meeting may be considered a cinematographic work. This includes any work expressed by any process analogous to cinematography, whether or not accompanied by a soundtrack.

Recording of sounds — whether music, speech, or other audio — is protected under the *Copyright Act*.[37] This protection is separate from the rights in the underlying musical or literary works that may be captured in the sound recording. The sound recording is a recording consisting of sounds fixed in any material form, "but excludes any soundtrack of a cinematographic work where it accompanies the cinematographic work."[38] This means that a recording of sounds that constitutes a soundtrack accompanying a cinematographic work, such as, for example, a motion picture, does not fall within the definition of a "sound recording."[39] The recording file fixes sounds made during the meeting in a computer file, so that the sounds are not merely fleeting or transitory, which can help attract copyright protection to the sound recording.

The *Copyright Act* also extends rights to a performer's performance. A recording may capture a performance and be subject to performer's rights, which include the sole right to communicate and reproduce the work.[40]

Copyright also protects collective work by different authors, compilations, and joint works of authorship. A recording that incorporates different copyright works may be considered a compilation, collective work or joint work of authorship. A compilation is a work resulting from the selection or arrangement of different works or data.[41] A collective work is any work written in

---

[36] *CCH Canadian Ltd. v Law Society of Upper Canada*, 2004 SCC 13 ["*CCH*"].
[37] *Copyright Act*, R.S.C., 1985, c. C-42.
[38] *Public Performance of Sound Recordings, Re,* 2012 SCC 38 at para 35 ["*Public Performance*"].
[39] s.2, *Copyright Act*.
[40] s.15, 26, *Copyright Act*.
[41] s.2, *Copyright Act*.

distinct parts by different authors or in which works or parts of works of different authors are incorporated.[42] A work of joint authorship means a work produced by the collaboration of two or more authors in which the contribution of one author is not distinct from the contribution of the other author or authors.[43]

Accordingly, a recording can involve different copyright works and trigger different protected rights. The recording file provides an accurate record of copyright works shared during the meeting and the associated contributor. This is helpful, as the recording can be reviewed to identify those works and clarify the owner to confirm or obtain permission before sharing and copying a recording. This may be more onerous if there are many attendees and multiple works captured. Participants should not contribute works of others to meetings unless they have permission to do so.

Transcript

The transcript of a meeting is generally verbatim text of the spoken words of the virtual meeting. *Gould Estate v. Stoddart Publishing Co.*[44] considered copyright in relation to a reporter's recorded conversations, and her "notes or report." The court concluded that the reporter had copyright protection in the notes and report.[45] However, a person who is merely a scribe or amanuensis that is writing an article from the dictation of another generally cannot claim copyright in the works.[46]

The speakers (performers) may also try to claim copyright. However, for copyright to subsist in a work, it must be expressed in material form and have a permanent endurance."[47] A person's oral statements in a speech, interview or conversation may not be recognized as literary creations to attract copyright protection.[48] However, as noted above, the recording of the statements fixes those oral statements in a material form, the recording file, so that they are not merely fleeting and transient. This helps protect those oral statements as copyright works.

Even if a transcriber did have a claim to copyright in the transcript for virtual meetings, for transcripts generated by AI software, the transcriber would be the AI software. If the AI program can be analogized to the scribe who is merely dictating the speech from the meeting participants, then copyright may not protect the transcription itself.

Canadian law is unsettled as to whether an "author" under the *Copyright Act* must be human.

The *Copyright Act* refers to a "natural person"[49] in relation to the author or maker.

There is an ongoing case before the Federal Court of Canada challenging a Canadian copyright registration that names an AI application as a co-author. In December 2021, the Canadian Intellectual

Property Office (CIPO) registered a copyright for *The Starry Night*-inspired image titled *Suryast*.[50] The copyright registration lists the RAGHAV Artificial Intelligence Painting App (RAGHAV) and Mr. Ankit Sahni as co-authors. In July 2024, the Samuelson-Glushko Canadian

---

[42] s.2, *Copyright Act*.
[43] s.2, *Copyright Act*.
[44] *Gould Estate v. Stoddart Publishing Co.*, 1996 CanLII 8209 (ONSC), aff'd 1998 CanLII 5513 (ONCA) ["*Gould Estate*"].
[45] *Ibid*, at para 30.
[46] *Ibid*.
[47] *Ibid*, at para 29.
[48] *Ibid*, at para 30.
[49] s.5(1)(b)(ii), *Copyright Act*.
[50] *Suryast* – Canadian Copyright Database.

Internet Policy and Public Interest Clinic (CIPPIC) filed an application in the Federal Court of Canada to challenge the copyright registration for *Suryast* and seek expungement of the copyright or removal of RAGHAV as a co-author.[51] CIPPIC argues that *Suryast* does not meet the originality requirement for copyright, and an AI system cannot be an "author" under the *Copyright Act*.

CIPPIC submits that Mr. Sahni merely providing three inputs to RAGHAV: a base image, a style image, and a value for how strong to apply the style image to the base image is a purely mechanical process that involved no human skill or judgment. CIPPIC further contends that "author" in the *Copyright Act* only includes a natural person (i.e., "human being"), and an AI system cannot exercise the common intent required for joint authorship.

While it is still unclear under Canadian law if AI authorship and AI-assisted authorship will attract copyright protection, the Canadian government launched a consultation[52] (which ended on January 15, 2024) to solicit input on authorship of AI-generated works. The consultation discusses that although the *Copyright Act* does not explicitly define the term "author," Canadian copyright jurisprudence suggests that "authorship" must be attributed to a natural person who exercises skill and judgment in creating the work, reflective of the fact the *Copyright Act* ties the term of protection to the life and death of an author.[53]

Considering the varying degrees and aspects of human contribution in the development and use of AI software, the authors (and therefore the initial owners) of AI-generated or AI-assisted works (e.g., AI developer, deployer, or user) remain an open question. A human could contribute sufficient skill and judgment in a work produced with the assistance of AI technologies to be considered the author of an original work. However, it is unlikely that this requirement would be met for works produced by generative AI systems, based solely on short simple prompts by human users.

Transcripts may be considered derivative works. Can the transcript be copyright protected if an AI program is used to generate a work? In *Oakcraft Homes Inc. v. Ecklun* [Oakcraft][54] an architect utilized computer aided design (CAD) software during his design process to create architectural drawings. The court concluded that the drawings created using the CAD software were copyright protected.[55] In *Oakcraft*, the architect used human skill and judgment in the design process. If a person is applying skill and judgment while using an AI tool to generate a transcript then this may be sufficient to afford copyright protection to the transcript.

Even if the transcript is not protecting by copyright, the written record provides an accurate account of what was discussed during the meeting and of other copyright works shared during the meeting. Participants can revisit the transcript to clarify details, confirm contributors, or review complex works.

If it is important to have copyright protection in a meeting transcript, then a human can review and summarize the transcript using its skill and judgment to generate a new original summary. The resulting original human-created summary would be protected by copyright given it involved human skill and judgment.

---

[51] *SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY ET AL v. ANKIT SAHNI* Court file no. T-1717-24.
[52] Government of Canada - *Consultation Paper:* Consultation on Copyright in the Age of Generative Artificial Intelligence.
[53] *CCH, supra* note 33 at para 25.
[54] *Oakcraft Homes Inc v Ecklund*, 2013 CanLII 41981 (ONSCSM) ["*Oakcraft*"].
[55] *Ibid*, at para 49.

Ownership and infringement

If meeting recordings and transcripts are protected as copyright works, then only the owner of these works can permit reproduction, usage and distribution. Reproduction, usage and distribution of copyright works without the owner's consent may amount to infringement.

If there is copyright in the recording and/or transcript then who owns the copyright and whose permission is required?

Generally, the owner of copyright is the author or maker subject to any existing agreements.

A recording may involve multiple copyright works, which complicates ownership as the author/owner of each individual work must be considered. Owning copyright in the recording does not automatically grant the right to use or reproduce any underlying works that may be captured in the recording as there may be different owners for underlying works.

The author or "maker" is presumed to be the owner unless the contrary is proved.[56] The "maker" of a cinematographic work is the person by whom the arrangements necessary for making the work are undertaken.[57] The person who undertakes the act of organizing the meeting and pressing record during the meeting may be the maker, as he or she undertakes the arrangements necessary for making the recording. This may be the meeting's "host" for example. If it is desirable to own the meeting recording, then it may be important to be the host of the meeting to increase the likelihood that you are considered the maker of the work or the recording and thus the owner.

The owner of performer's rights is typically the speaker, and if there are underlying works in the recording and transcript then they may be owned by the authors of those works.

For a sound recording, a maker means the person by whom the arrangements necessary for the first fixation of the sounds are undertaken. The creator of the sound recording is typically the first owner of copyright in the recording, unless there is an agreement stating otherwise.

Performers whose performances are fixed in a sound recording also have certain rights under the *Copyright Act*.

Collective works may be jointly owned by the different authors.

The owner of any copyright in the recording may be different than the owner of copyright in other original work captured by the recording. That is, ownership of the copyright in the recording does not automatically amount to ownership of any works captured in the recording.

Fortunately, the meeting recording provides an accurate and useful account of what works were shared or contributed during the meeting that can be reviewed to clarify ownership and required permissions.

However, even if individuals shared or contributed work during the meeting, they may not be the owner of the work and may not have the ability to grant permissions for the work.

If the authors are employees, then they may have an employment agreement transferring ownership of any work they author to the employer. Further, if the work was made in the course

---

[56] *Canadian Broadcasting Corporation v. Conservative Party of Canada*, 2021 FC 425 at para 33 ["*Canadian Broadcasting*"]; s.34.1(1), *Copyright Act*.
[57] s.2, *Copyright Act*.

of employment, then the employer is deemed the first owner of the work in the absence of any agreement to the contrary.[58] If there are multiple authors with the same employer, then that employer would own the works by those authors including any joint works.

If the meeting is recorded by employees as part of their jobs, then typically the employer would be the owner of recording or works involved in the recording.

If there are different authors of works involved in the recording and those authors are employed by different employers, then ownership may be distributed across those different employers/authors.

Ownership and usage rights of the works involved in the recording may be clarified in a written agreement between the employers and participants.

Copyright gives the owner the exclusive right to reproduce, publish, and communicate the recording to the public. Sharing or publishing the recording without proper authorization may infringe copyright.

Owning copyright in a recording does not automatically grant the right to use or reproduce the underlying works unless permission is obtained from the owners of any works captured therein. Distributing a recording of a virtual meeting and the transcript may infringe on the copyright of the owner (e.g., participants or third parties) of the underlying works if permission is not obtained. Further, distributing any presentations, documents, or other materials shared during the meeting may infringe on the copyright of the owners of the copyright in those shared materials.

There are limited exceptions to infringement under the *Copyright Act* allowing certain uses of copyright works without the need for permission from the copyright owner. For example, fair dealing allows the use of works for purposes such as research, private study, criticism, or review. Whether the use is fair depends on various factors such as the character, purpose, nature of the work, amount, alternatives, and effect on the market. There are also exceptions for education institutions, private purposes, technological processes, accessibility, and so on. The context of the meeting and usage of the recordings should be considered to determine whether exceptions apply.

The meeting recording and transcript can be reviewed to identify all works and the associated contributor and owners. Permission from the copyright owner(s) should be obtained before sharing and copying the meeting recording and transcript if an exception does not apply. The recording file provides an accurate record to provide evidence of the works and the associated contributor or author of those works. This can help with legal compliance and obtaining permission by those contributors if needed.

Moral rights

The author has moral rights that include the right to the integrity of the work and the right to be associated with the work (or remain anonymous). Authors of works presented in meetings retain moral rights, including this right to be credited and to object to derogatory treatment of their work if it impacts the integrity of the work, even if copyright is assigned. Moral rights cannot be assigned and can only be waived. If moral rights in any original works involved in the recordings or transcripts are not waived by the author, then those moral rights should be respected to avoid infringement. The waiver of moral rights can be made by the authors during the meeting and

[58] s.13(3), *Copyright Act*.

captured by the meeting recording, for example. The waiver can also be obtained in a separate legal document before or after the meeting.

Other types of IP embodied in the recording or transcript

A participant might share information about a patentable invention or design drawings during the meeting that may be captured in the recording and transcript. Accordingly, content embodied in the recording or transcript may include a patented invention or protected design. The content may also include subject matter that will form part of a patent application. Typically, the invention is owned by the inventor subject to existing agreements (e.g., employment agreement, IP agreement assigning invention/patent rights to a third party).

Under patent law, the date the invention became available to the public is a relevant consideration for patentability. The subject matter of a patent is often confidential until the patent publication. The subject matter may be disclosed in a non-confidential virtual meeting and captured in the recording. This may be a trigger event under patent law, and the owner of the invention or design should consider this disclosure and any confidential obligations as part of its patent strategy. Further, the owner of the recording is not automatically the owner of the patented invention or protected design captured in the recording. Instead, the inventor or designer is the first owner subject to existing agreements. Permission of the owner is required to make, use or sell the invention.

The meeting recording provides an account of what was discussed during the meeting that can be reviewed to clarify whether any patentable subject matter was indeed shared during the meeting and by whom. This can help avoid misunderstandings and disputes about what was disclosed and by whom. The meeting recording should be reviewed before the potentially patentable subject matter is used or filed in a patent application. The meeting recording also provides a record of the disclosure that can be later assessed to determine whether it was indeed confidential or considered a public disclosure, and whether the content disclosed is indeed an enabling disclosure as set out in the relevant patent law.

Proper management of IP within virtual meetings ensures that rights are respected, avoiding legal complications and fostering a secure environment for sharing innovative ideas and creations.

Managing IP during meetings and recordings requires clear communication, proper documentation, secure handling of recordings, and compliance with legal requirements. Permissions and agreements are essential to avoid infringement and disputes, particularly when the participants are employed by different entities.

Provide advance notice to participants that you will be creating a meeting recording. A disclaimer can be displayed or read at the start of the meeting reminding participants not to share or display any copyrighted material unless they have obtained the necessary permissions or an exception applies. Discuss and, if possible, confirm in writing the ownership of any IP generated during the meeting. If relevant, have participants sign IP assignment or confidentiality agreements before or after the meeting. Mark the recording itself with a copyright note to give notice of ownership and help prevent misuse.

Meeting recordings provide accurate evidence for establishing authorship, inventorship, agreements, and permissions. Meeting recordings can serve as evidence of who contributed specific ideas, inventions, or works during discussions. This can be helpful in establishing authorship or inventorship in the event of a dispute.

Recordings provide an accurate (timestamped) record of when something (including an invention) was first discussed or conceived. This can be important for establishing priority in patent law (e.g., proving who was first to invent or disclose an idea) or in copyright disputes. The meeting recording can be reviewed to identify the different works, and the associated contributors and authors. Permission to use and share the works can be obtained from the owners to avoid infringement.

If participants agree to assign rights or provide permission to use IP during a meeting, the recording can serve as evidence of these agreements. This is especially useful if written documentation is lacking or ambiguous. However, follow up the meeting with written document confirming the rights or other permissions granted during the meeting.

In collaborative projects, recordings can help clarify the contributions of each participant, to help resolve disputes about shared IP rights, joint authorship or inventorship. Ideally, any ownership and licensing of IP is determined before the collaborative meeting to avoid unintended consequences and misunderstandings.

A meeting recording may provide evidence of how the work or invention was developed or obtained, and by what participant. The meeting recording can be used to show that something was independently developed, rather than copied.

The following Governance and Best Practices section provides additional guidance to help protect valuable IP, clarify ownership, and reduce the risk of disputes or unauthorized disclosures.

D. Confidentiality

In some situations, audio or video recordings and transcripts of virtual meetings can contain confidential information. Recording and transcribing such confidential information without consent may be a breach of confidence under tort law. Misuse of confidential information may also breach agreements with confidentiality obligations. Not protecting the recordings and transcripts and enabling access by others to the files (that contain the confidential information) that were not securely stored may also breach confidentiality.

In Canada, confidential information is protected by tort law. A breach of confidentiality occurs when confidential information is disclosed or misused in violation of a duty of confidentiality. Entities often exchange confidential information when participating in projects, collaborations or licensing agreements. Further, professional service providers who are independent contractors can receive confidential information from clients (e.g., lawyers, consultants, engineers). Often contracts are in place between these entities with provisions that govern use of confidential information. Accordingly, contract law is also often relevant to confidential information.

Under tort law, the duty of confidentiality arises when someone has been given information with the understanding that it will be kept confidential. Even without a contract, the duty of confidentiality may still apply. The Supreme Court of Canada (SCC) in *Lac Minerals Ltd. v. International Corona Resources Ltd.* ["Lac Minerals"],[59] considered Lac's, a mining company, use of information about gold deposits disclosed to them in confidence by Corona, another company.

---

[59] *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 SCR 574 ["*Lac Minerals*"].

According to *Lac Minerals*, the three criteria in determining whether there is a breach of confidence are:

1. The information itself must have the necessary quality of confidence about it.
2. The information must have been communicated in circumstances importing an obligation of confidence.
3. There must be misuse or unauthorized use of that information to the detriment of the party communicating it.

What information is confidential and why it is classified as confidential must be identified precisely.[60]

As an example, in *Lac Minerals*, Corona shared confidential information about gold deposits with Lac that Lac ultimately exploited to win a bid on a property, which Corona was not aware of. The additional material private information shared by Corona was valuable to evaluate the property in question, and Corona only shared the confidential information with Lac under the assumption that there would be a business arrangement or joint venture between the two companies in the future. Lac exploited this confidential information for its own gain, at the expense of Corona.

To supplement the elements identified in *Lac Minerals*, the SCC in *Cadbury Schweppes Inc. v FBI Foods Ltd.* [Cadbury][61] clarified the type of information that can be considered confidential through the "Springboard Doctrine." The Springboard Doctrine recognizes that gaining information from public sources may save a defendant substantial time, effort and costs in searching for, gathering, and obtaining the information themselves and, therefore, may be regarded as confidential even though the defendant could have collected it from sources available to the public. The information is viewed as having provided the defendant with a "springboard" and has some value because it has given the defendant a head start in the endeavor.[62] In these situations, the party whose confidential information was used may claim additional damages for lost profits due to the resulting competition from using the confidential information.

In the *Cadbury* case, the dispute was around manufacture of two similar beverages. The factual evidence indicated that access to Cadbury's confidential formula for a kind of beverage through a license agreement enabled FBI to bring its own competing product to market about one year sooner than it could otherwise have done without Cadbury's confidential information. Accordingly, the SCC awarded damages of one year's worth of profits lost by Cadbury due to the competition that resulted from FBI's use of Cadbury's confidential information.

The duty of confidentiality also arises from contract law when a contract between parties includes confidential requirements. If a virtual meeting involves content considered "confidential information" in a contract between the participants (extending to entities the participants are representing) then those contractual requirements are applicable to the recording and transcript that incorporates the confidential information.

For example, the recordings and transcripts may only be used for particular purposes and may need to be protected from access by others to avoid breaching contractual requirements. Further, if a participant in the virtual meeting has other confidential contractual obligations (e.g.,

---

[60] *Dymon Storage Corporation v. Nicholas Caragianis*, 2022 ONSC 5883.
[61] *Cadbury Schweppes Inc. v. FBI Foods Ltd.*, [1999] 1 SCR 142 ["*Cadbury*"].
[62] *Cadbury*, paragraph 67.

employment agreements requiring employees to keep company information confidential), the participant would be held accountable to those separate confidential requirements as well. For example, an employee may not be permitted to share an employer's confidential information outside of the company, which would extend to not being permitted to share the employer's confidential information in a virtual meeting involving participants outside of the company.

The type of information to be considered confidential can be explicitly worded and described in a contract. However, even with a contract, it may be difficult to describe the confidential information comprehensively and precisely. For example, in Cadbury, there was a written contract in the form of a licensing agreement that specifically prohibited using a specific clam broth by the defendant once the license had expired, but did not specify what else was prohibited as part of the confidential information because it depended on confidential formulas. Note that comprehensive agreements and contracts can also allow parties to contract out of their duties of confidentiality and other obligations regarding confidentiality. A contractual term that deals expressly or by necessary implication with confidentiality can limit or negate the general expectation of a party's duty of confidentiality.

There may be some exceptions to the duty of confidentiality that arise when public interest or legal requirements outweigh the need to protect sensitive information. For example, a valid court order or subpoena could compel disclosure of confidential information in legal proceedings. Another example of an exception to the duty of confidentiality is when a party provides a waiver to explicitly or implicitly authorize the disclosure of confidential information.

Recordings can be useful to demonstrate that reasonable steps were taken to protect confidential information discussed in meetings. Recordings also provide evidence of what confidential information was discussed during the meeting and by whom. The recording can also provide a record to demonstrate that participants agreed to maintain confidentiality of what was shared during the meeting. Notify meeting participants before disclosing any confidential information to confirm that all participants are obligated to keep the information confidential. Ideally, there should be a confidential agreement in place before the meeting and any disclosure of confidential information. Otherwise, follow up with a written agreement to confirm the confidential obligations that were agreed to during the meeting.

E. Regulatory compliance

Financial services industry

Organizations operating in the financial services industry must account for sector-specific legal and regulatory obligations when using meeting productivity tools that enable recording and transcription. For example, investment dealers are subject to recordkeeping requirements that apply to communications relating to trades, orders, and client instructions. These requirements are technology neutral and extend to electronic formats, including meeting recordings and transcripts, provided they are retrievable, legible, and secure.

While there is no blanket requirement to record all calls or meetings, organizations in the financial services industry often choose to do so for compliance, auditability, and dispute resolution purposes. If a meeting involves the provision of advice, instructions, or decisions related to client accounts or financial products, the resulting recording or transcript may be considered part of the firm's official books and records and should be retained accordingly. If a transcript is to be used in this capacity, it should be reviewed and approved by one of the meeting attendees to ensure it reflects the exchanges that took place.

Canada's Office of the Superintendent of Financial Institutions (OSFI) requires federally regulated financial institutions (FRFIs) to ensure the protection of all data (including meeting transcripts or other meeting recordings). Where data is processed by third-party service providers, FRFIs must ensure such data remains subject to the same standards as those employed by the FRFIs themselves, in particular with respect to the confidentiality, integrity, and availability of such data.

Beyond compliance, recording and transcription tools offer significant operational benefits. They can improve documentation accuracy, reduce reliance on manual note-taking, and support the generation of client summaries and follow-up actions. Recording and transcription tools can assist in extracting key insights from meetings, enhancing client service and internal collaboration. These features also support training, quality assurance, and internal audits, helping organization maintain high standards while reducing administrative burden. When used appropriately, they can strengthen transparency and trust with clients, while also improving regulatory readiness.

Healthcare sector

Organizations operating in the healthcare sector must navigate a complex regulatory landscape when using meeting productivity tools that enable recording and transcription. For example, Ontario's *Personal Health Information Protection Act* (the Ontario *PHIPA*)[63] imposes a requirement on healthcare providers and health information custodians leveraging videoconferencing platforms to take steps to proactively protect patient security and privacy in accordance with such act. The Ontario *PHIPA*, the Alberta *HIA* and Quebec's health privacy legislation[64] also impose additional obligations for qualification requirements for professionals delivering telehealth services, which now commonly include videoconferencing capabilities.

Clinical encounters, whether in-person or virtual, may involve the collection of personal health information, which is subject to federal and provincial privacy legislation as discussed in Section A. Due to the sensitive nature of the information discussed in these meetings, healthcare providers should obtain meaningful and express consent prior to recording or transcribing any patient interaction. This includes clearly explaining the purpose of the recording, how it will be used, and whether it will be stored or shared. In some jurisdictions, written consent may be required, and institutions may have internal policies governing the use of recording technologies. If recordings or transcripts are used to generate clinical documentation, providers must review and validate the content to ensure accuracy and avoid introducing errors into the patient's medical record.

When implemented with appropriate safeguards, these tools can offer substantial benefits to healthcare organizations. Transcription can streamline clinical documentation, reduce administrative workload, and improve the accuracy of patient records. Recordings can support continuity of care, enable peer review, and serve as valuable training material for medical staff. AI-powered summarization can assist in identifying key clinical decisions and follow-up actions, enhancing care coordination. These features can also improve patient engagement by providing clearer communication and documentation of care plans. Used responsibly, they contribute to better outcomes and more efficient healthcare delivery.

---

[63] *Personal Health Information Protection Act, 2004*, SO 2004, c 3.
[64] *Act respecting health and social services information and amending various legislative provisions,* CQLR, R-22.1.

Accessibility standards and requirements

The *Accessible Canada Act* (ACA),[65] requires that video conferencing services are inclusive, including by providing support using assistive technologies, ensuring that platforms are capable of being navigated by individuals with disabilities, including with respect to using sign language interpretation, captioning, and transcription.

At the provincial level, legislation such as Ontario's *Accessibility for Ontarians with Disabilities Act* (AODA)[66] requires that videoconferencing used by organizations be accessible to individuals with disabilities. Manitoba,[67] Nova Scotia,[68] and British Columbia[69] have similar legislation in place.

There are many productivity tools designed to make meetings more efficient or accessible for users. These tools can offer meaningful benefits for individuals living with a disability. For example, bots such as meeting assistants, virtual meeting reporters, or AI note-takers can attend meetings on behalf of participants, take notes, and draft summaries, potentially capturing sensitive information in the process. At the same time, features such as live captioning of spoken words can act as barrier-removal tools for individuals with hearing challenges, enhancing inclusivity and supporting compliance with accessibility standards.

F. Litigation and disputes

A potential benefit to recording or transcribing meetings is that the recording or transcription could be a persuasive piece of evidence when attempting to resolve a dispute or in future litigation. For example, when assessing credibility of witnesses, the court will often look to contemporaneously created documents to assess whether a particular witness is credible.[70] Videos or recordings can be particularly persuasive, as they may be less prone to accuracy issues than transcriptions (as discussed below) and may convey more information than a transcription (such as tone for example).[71]

That said, the creation of a recording or transcription may lead to disclosure obligations (regardless of whether the recording party would otherwise want to disclose) and would be subject to admissibility requirements (which would need to be met before the recording party can rely on them in litigation).

Document Disclosure Requirements

Depending on the rules of the relevant court or procedures of the relevant decision-maker, transcripts, sound recordings, video recordings, as well as electronic data from virtual meeting software that is relevant to the matter in question may fall within the scope of document production in a legal proceeding. If so, then in certain jurisdictions there would ordinarily be a mandatory requirement to produce the information to other parties in the litigation, even if it does not assist the recording party's case or position.

For instance, in British Columbia, the *Supreme Court Civil Rules*[72] (the BCSC Rules) require that each party of record to an action prepare a list of documents after the end of the pleading period

---

[65] *Accessible Canada Act*, SC 2019, c 10.
[66] *Accessibility for Ontarians with Disabilities Act, 2005*, SO 2005, c 11.
[67] *Accessibility for Manitobans Act*, CCSM, c A1.7.
[68] *Accessibility Act*, SNS 2017, c 2.
[69] *Accessible British Columbia Act*, SBC 2021, c 19.
[70] *Faryna v Chorny*, [1952] 2 D.L.R. 354 at para 10 (BCCA).
[71] See e.g., *R. v. Nikolovski*, [1996] 3 SCR 1197 at paras. 19-23.
[72] *Supreme Court Civil Rules,* BC Reg 168/2009.

that sets out "all documents that are or have been in the party's possession or control and that could, if available, be used by any party of record at trial to prove or disprove a material fact."[73] In addition to material documents, parties may also demand, and the court may order, the production of a broader range of documents that simply "relate" to the matters at issue.[74] The definition of "document" in the BCSC Rules includes videos and recordings of sound,[75] and has also been interpreted expansively to include electronic data stored on a computer's hard drive.[76]

Similarly, the *Ontario Rules of Civil Procedure*[77] (the Ontario Rules) contain a similar, non-exhaustive definition of "document" that includes sound recordings and videotapes for the purposes of Rule 30, pertaining to discovery of documents. That said, any use of the records by parties receiving such disclosure would similarly be subject to the relevant rules, including any implied or deemed undertaking to not use such records for any purposes other than those of the proceeding in which the evidence was obtained unless a permitted exception to such undertaking applies.[78]

While worded slightly differently, the predominant consideration for document disclosure in both the BCSC Rules and the Ontario Rules is ultimately the record's relevance to the matter at hand. If that threshold of relevance is met, then the requirement to list and produce the record is likely triggered unless narrow exceptions to disclosure are engaged. For example, while privileged documents (such as a meeting with counsel to discuss legal advice) are usually exempt from disclosure, confidential documents (such as *in camera* meetings) are not necessarily exempt from disclosure. Neither set of rules distinguishes between the nature or type of record in the requirement to disclose – once created, a recording would be subject to the same requirement to disclose as a transcript and vice versa, if the contents of that recording or transcript meet the threshold of relevance for production.

Document disclosure requirements can vary from jurisdiction to jurisdiction. For instance, while parties to legal proceedings in Quebec also need to produce, within prescribed time limits, the exhibits supporting their pleadings and the evidence they intend to use at trial,[79] and have a general obligation to cooperate and keep one another informed at all times of the facts conducive to a fair debate,[80] parties are not required to automatically provide one another with a list of all relevant documents in their current or past possession. However, parties to legal proceedings in Quebec may nonetheless be faced with different types of requests to provide documents targeting recordings and transcripts in their possession. In such cases, they would be required to produce all such documents, subject to applicable objections.

It is worth noting that in some jurisdictions, such as British Columbia,[81] parties are required to list material documents that have been in their possession or control in the past, even if they are no longer in their possession and control. This could, depending on the case, mean that a recording party is required to disclose, by listing them, that recordings or transcripts have been deleted. This is not the case in all jurisdictions – for instance, in Quebec, parties are not required to list material documents that have been in their possession or control in the past.

---

[73] *Supreme Court Civil Rules*, R. 7-1(1).
[74] *Supreme Court Civil Rules,* R. 7-1(11).
[75] *Supreme Court Civil Rules*, R. 1-1(1).
[76] *Bishop v Minichiello*, 2009 BCSC 358 at paras. 46 and 57 ["*Bishop*"].
[77] *Rules of Civil Procedure,* RRO 1990, Reg 194 [the "Ontario Rules"].
[78] See for instance Rule 30.1, the Ontario Rules.
[79] *Code of Civil Procedure,* CQLR c. C-25.01, art. 247 and 248.
[80] *Code of Civil Procedure,* CQLR c. C-25.01, art. 20.
[81] *Supreme Court Civil Rules*, R. 7-1(1).

As such, the volume of records that may be caught by a litigation hold and document disclosure obligations can be significantly expanded (along with associated costs with reviewing and even storing the data in question) if an organization makes a record of a meeting that relates to subsequent litigation. Organizations who intend to use such functions would be well served to (a) consider whether the meeting in question would benefit more from a recording, a transcription, or both, taking into account considerations such as the format of the meeting (will there be just one speaker, or multiple speakers?), topics for discussion in the meeting, the number of attendees, the length of the meeting, and whether someone is available post-meeting to review the recording or transcription, and (b) review their data retention policies to ensure the policy content sufficiently addresses how recordings or transcriptions of meetings are maintained.

Accuracy and completeness of records

While recording and transcription tools are highly beneficial in terms of the automated support they can offer to meeting participants, due to user error or other unavoidable or unanticipated issues, recordings and transcriptions are not necessarily infallible in all circumstances.

For instance, AI transcription may not have a 100% accuracy rate in capturing the meeting discussion, particularly where there are more than two participants who may be speaking at the same time. The transcription may attribute spoken statements to the wrong speaker, miss portions of a statement, or misinterpret a word for another. Such errors may not be caught by the meeting organizer and corrected at the time of transcription, thus resulting in either the mistaken belief that there is an accurate record of said meeting (which ultimately is not accurate) or the possibility of an inaccurate transcript being produced in a legal proceeding. If an organization only discovers there was an error in the recording or transcription long after the meeting in question occurred, memories of the participants may have faded by that time, making it difficult to secure reliable oral evidence on the actual conversation that took place. As such, recordings or transcriptions of meetings of particular importance would benefit from a fairly immediate review by a participant to ensure accuracy.

Regarding any applicable document disclosure requirements, the that a transcription is inaccurate would not normally exempt it from production, if the transcription is otherwise producible. Should a party to litigation discover that a relevant transcript in its possession or under its control contains errors, it should consult with legal counsel. In certain circumstances, it may be appropriate to produce that transcript, along with the relevant audio and/or visual recording (if one was made), with an explanatory note to the other parties to the litigation, but this may vary case by case and jurisdiction by jurisdiction.

An organization may be a party to litigation where another party produces as part of document disclosure, or attempts to introduce into evidence, a recording or transcript of a meeting involving representatives of the organization that is incomplete, inaccurate, or even edited (whether intentional or not). In such cases, the organization will likely wish to press the disclosing party on these issues. For example, this can involve questioning the representative of that party who is introducing the document either in an examination for discovery or on the stand, and raising an objection to an attempt by a party in that litigation to admit such records into evidence on the basis of concerns regarding accuracy, completeness, authenticity, or reliability.

In some jurisdictions, potential issues with inaccuracy may pose a problem for the admissibility of the recording. In Quebec for example, proof of authenticity is required for real evidence to have probative value.[82] In other jurisdictions, the courts have taken a more flexible approach and

[82] See for instance *Civil Code of Quebec*, CQLR c. CCQ-1991, art. 2855.

concluded that there is not necessarily an obligation to prove that a recording has not been altered and a video is admissible as long as it provides a substantially accurate and fair representation of the recorded events.[83]

In the case of recordings, authenticity issues may be prevented by the production of the file's metadata, which may be deemed sufficient to attest the authenticity of technological recordings if the metadata identifies sufficient information such as the author, the date of creation, and any modifications to the file (or lack thereof).[84] Authenticity may also be proven by testimony or through other evidence, but it is a good practice to preserve and produce the metadata along with the recording. In the case of automated transcripts, it would likely be difficult to demonstrate their integrity and authenticity without the corresponding recording. An automated transcript should ideally be produced as an accessory to a recording, as a tool for the parties and the adjudicator of the legal proceeding.

Introduction of surreptitious recordings into evidence

Another possible challenge to the admissibility of recordings/transcriptions of meetings as evidence in legal proceedings relates to the admissibility of surreptitiously obtained recordings or transcriptions. The question of whether such a recording or transcription is admissible can turn on the individual circumstances, including whether the situation was such that the surreptitious recording was warranted. In determining whether a relevant recording or transcription should be excluded, adjudicators will also weigh its probative value against any prejudicial effect.[85]

The ability to introduce such a recording or transcription into evidence has the potential of determining the course and outcome of litigation.[86] For instance, in the labour arbitration setting, if an employer is unable to adduce a recording capturing a grievor's misconduct on the basis that collection is found to be improper, it may lose the necessary evidentiary support for any discipline imposed as a result of that misconduct.

Restrictions on recording proceedings

While dependent on the jurisdiction and forum, courts and decision makers will very likely also have rules of procedure restricting the creation of audio or video recordings or transcripts of proceedings, including those that are held virtually.[87] Counsel and parties must ensure their compliance with such rules and seek an exemption from the adjudicator if one is necessary.

Privilege considerations

As noted above, privileged information has special protections in litigation and is not normally subject to disclosure obligations. The question of whether information is privileged will be contextual, but privileged information may include, for example, a meeting in which legal advice is conveyed or a meeting to discuss how to respond to a legal claim. That said, this protection is lost where privilege is waived, and privilege can be waived where the information is not kept confidential. For example, if a recording or transcript of an otherwise privileged meeting is saved

---

[83] See e.g., *R. v. Bulldog*, 2015 ABCA 251 at paras. 26 – 33.
[84] *Benisty c. Kloda*, 2018 QCCA 608, paras. 99 to 105.
[85] For the rule in Quebec, see *Civil Code of Quebec*, CQLR c. CCQ-1991, art. 2858.
[86] For an example in Quebec, see *Bellefeuille c. Morisset*, 2007 QCCA 535.
[87] For instance, see the Policy on Use of Electronic Devices in Courtrooms, effective date September 17, 2012, setting out the permitted and prohibited use of electronic devices in courtrooms of the Court of Appeal, the Supreme Court and the Provincial Court of British Columbia: <https://www.bccourts.ca/supreme_court/media/PDF/Policy%20on%20Use%20of%20Electronic%20Devices%20in%20Courtrooms%20-%20FINAL.pdf>; See also the Quebec Superior Court policy, effective date: May 22, 2025 Lignes directrices visant à encadrer l'utilisation des technologies en salle d'audience et la conduite des participants qui se joignent à distance à une audience.

in a location that is generally accessible to third parties or shared or forwarded to third parties, then privilege may be waived.

Organizations who intend to make records of meetings would be well served (a) to adopt a policy of not recording meetings that contain privileged content, or (b) if such recordings are made, adopt a policy that would ensure the recording is kept in a confidential location and is clearly marked as being privileged.

G. Other legal considerations

Human Rights laws

Videoconferencing platforms that leverage AI (for example, those with facial recognition, emotion detection, automated decision-making (such as access control and participant prioritization) capabilities must comply with the *Canadian Human Rights Act* (CHRA),[88] and provincial counterparts such as the *Ontario Human Rights Code* (OHRC)[89] and Quebec *Charter of Human Rights and Freedoms*[90] prohibit discrimination on the basis of race, gender, disability and other protected grounds. If AI-enabled videoconferencing systems treat people unfairly due to algorithmic bias, such treatment could form the basis of a legal complaint under such human rights legislation.

Canadian Criminal Code

As noted above, section 184 of the *Criminal Code*[91] prohibits the intentional interception of private communications using any device unless one party to such communications consents. This is relevant in the context of videoconferencing that contains AI features such as speaker recognition, automatic transcription, and any analysis of the speech or behaviour of videoconferencing participants.

Contracts and torts

Deployers of videoconferencing systems must clearly delineate liability terms in the applicable terms of use and end-user license agreements (EULAs), including careful consideration given to items such as indemnities, where potential harm is caused by an AI feature. Users of videoconferencing platforms must comply with such terms and conditions. Parties deploying and leveraging systems with meeting recording and transcription features must also bear in mind any potential duty of care that is owed to users of such systems.

Data Residency: Cross-border data transfers

Since many AI-enabled services (including videoconferencing) are connected to technology infrastructure that may be based outside of Canada, it is important to bear in mind that under *PIPEDA* and equivalent provincial privacy legislation, deployers of such systems must notify users if users' personal data is or will be processed outside of Canada. This is in addition to data residency requirements applicable to Canadian government data classified as "Protected B" and "Protected C" or classified at the federal level, as well as similar restrictions in place under Quebec legislation.

---

[88] *Canadian Human Rights Act*, RSC 1985, c H-6.
[89] *Human Rights Code*, RSO 1990, c H.19.
[90] *Charter of Human Rights and Freedoms*, CQLR, c. C-12.
[91] s.184, *Criminal Code* of Canada.

Law society requirements and guidance

In considering the recording or transcription of any conversations in their practices (including but not limited to using virtual meeting software), Canadian lawyers must adhere to relevant requirements imposed by their governing law societies.

For instance, the Law Society of British Columbia's Code of Professional Conduct and the Law Society of Ontario's Rules of Professional Conduct each prohibit lawyers from using 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.[92] A similar prohibition is suggested by the Federation of Law Societies of Canada in its *Model Code of Professional Conduct*.[93] In Quebec, even if there is no explicit prohibition in the *Code of Professional Conduct of Lawyers*,[94] a clandestine recording of a conversation, although legal in certain circumstances, may be perceived as a lack of courtesy and could be considered as a behaviour inconsistent with the honour, dignity or practice of the profession[95] and therefore, contravene the spirit of the *Code of Professional Conduct of Lawyers*.[96] This is also the position of the Barreau du Québec on this matter.[97]

Additionally, lawyers should be mindful of any guidance issued by their governing law societies on the use of AI more generally in legal practice. For instance, the Law Society of British Columbia has issued a practice resource on generative AI[98] that contemplates a lawyer's general duty of confidentiality and duty of candour will include obligations to fully disclose any use of AI as well as to obtain informed consent from the client for any use made of its private information. Similar guidance was issued by the Barreau du Québec.[99]

Inadvertent waiver of solicitor-client privilege

As noted above, organizations recording or transcribing meetings with counsel for the purposes of obtaining legal advice or in relation to pending or active litigation should take care to properly store and limit access to such records. Disclosure to, or access by, a third party to such records could result in an inadvertent waiver of the solicitor-client privilege attaching to those records.

Terms of service

Many virtual meeting platforms have terms of service that outline the rules regarding recording and sharing content. Users must adhere to these terms to avoid legal issues.

French Language requirements in Quebec

In Quebec, technological tools offered to employees should be made available to employees in French, under the Quebec *Charter of the French Language*.[100]

---

[92] Rule 7.2-3, Law Society of British Columbia, Code of Professional Conduct for British Columbia; Rule 7.2-3, Law Society of Ontario, Rules of Professional Conduct.
[93] Federation of Law Societies of Canada, "*Model Code of Professional Conduct,"* as amended April 2024, section 7.2-3.
[94] CQRL, c. B-1, r. 3.1.
[95] Quebec *Professional Code*, CQRL, c. C-26, section 59.2.
[96] *Code of Professional Conduct of Lawyers*, sections 4, 112 and 129.
[97] See *Barreau du Québec (syndic adjoint)* c. *Atudorei*, 2016 QCCDBQ 28.
[98] Law Society of British Columbia, "Practice Resource Guidance on Professional Responsibility and Generative AI," Accessed June 22, 2025: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/Professional-responsibility-and-AI.pdf>.
[99] Barreau du Québec, "L'intelligence artificielle générative: Guide pratique pour une utilisation responsable," Accessed August 26, 2025 : <https://www.barreau.qc.ca/media/bnddaqfd/guide-intelligence-artificielle-generative.pdf>.
[100] CQLR, c. C-11.

Governance and best practices

1. Internal virtual meeting policy

Companies should have a specific internal policy directed to employee use of virtual meetings, the recording and transcription of meetings, and usage of recordings and transcripts. A sample virtual meeting policy template is attached as Appendix A.

A company likely already has other internal policies relevant to the creation of transcripts and recordings using virtual meeting productivity tools, such as data protection policy, information security policy, confidentiality policy, acceptable use of technology policy, code of conduct/ethics, respectful workplace policy, mobile device security policy, and so on. These policies should be referenced in the virtual meeting policy for awareness, completeness, and consistency. These existing policies should be reviewed to see if any updates are required to address transcripts and recordings.

For example, organizations can update security policies to ensure they outline appropriate security safeguards as to how and where such recordings and transcripts are to be stored, including, but not limited to, encryption, proper access controls, appropriate physical security for devices, network security and antivirus software. As another example, organizations can update their privacy policies to ensure they clearly explain what data can be collected, how it will be used, whom it may be shared with, and how long it will be retained, especially when the collected data includes personal information obtained through the recording and transcription of virtual meetings. This privacy policy can include an electronic monitoring policy that sets out whether the employer or organization electronically monitors employees, including through the use of the recordings and transcripts, and if so, details of how and in what circumstances that monitoring occurs and the purposes for which the information collected may be used.

Any employee handling meeting recordings or transcripts must comply with the virtual meeting policy, any other relevant policies and applicable law.

The policy can be shared by a central source (e.g., HR, legal, IT) so that requests and questions can be centrally managed.

A company “town hall” or an employee meeting may be helpful to have discussions with employees about pressing concerns relating to virtual meetings (e.g., when to record, when not to record, consent rules/guidelines, administrative and sharing rights).

The virtual meeting policy (and other relevant policies) should be clearly communicated to employees and mandatory training can be provided to ensure employees understand the policy to support compliance. Offering mandatory training regarding usage of the meeting software/application can help ensure the employees understand the proper utilization of productivity tools, such as recording and transcripts, while abiding by the policies.

2. Approved platforms with training/support

Companies should only permit employees to use approved virtual meeting platforms for all work-related meetings. Companies should conduct diligence on the tools and vendor before approving the platforms to ensure they comply with applicable law and internal policies. This may involve an impact assessment to understand how data will be processed and stored, risks and mitigation strategies. Review applicable service agreements to determine security, location, accessibility of recordings and so on.

To support compliance, companies can provide mandatory training on approved virtual meeting tools (including, but not limited to, confidentiality training), and ongoing support and troubleshooting through the enterprise IT helpdesk should any employees have questions or inquiries about the virtual meeting tools.

3. Only for legitimate business purposes

All virtual meeting recordings and transcripts must be created, used, and retained only for legitimate business purposes. The user making any recording or transcript should clearly define the purpose of recording the meeting, and ensure all other participants are aware of the purpose of the recording. Examples of such purposes include facilitating internal communications, documenting key decisions, training and development, ensuring regulatory compliance, accessibility, and maintaining accurate records of essential discussions.

A company can keep a record of the purpose for which the recording and transcript will be used, and do not use them for any other purpose without further consent. Ideally, the company should only record or transcribe what is necessary for the stated purpose and avoid capturing unnecessary personal information.

If recordings and transcripts are to be used for secondary purposes, such as training AI models or improving algorithms, organizations should make these secondary purposes clear to participants, and additional consent requirements may be required for these secondary purposes. Any personal information should not be used beyond its original purpose without proper authorization to avoid regulatory penalties and reputational harm.

4. Transparency and documentation

A participant (or an organizer) of a virtual meeting should not record meetings without permission of other participants. Before any meeting is recorded or transcribed, ensure all participants are aware that the meeting will be recorded, transcribed, and analyzed. Obtain explicit consent before proceeding. For example, the organizer should inform attendees that the session will be captured, explain the rationale for doing so, and offer participants the option to raise concerns or, where legally required, to withhold consent if they have legitimate grounds.

A company should maintain records of consent, notices provided, and any permissions granted for the use of materials shared during the virtual meeting that may be captured in the recording or transcript. The organizer of a meeting should keep a written record of the notification and consent for the recording. Where possible, the meeting host or organizer should confirm the intention to record the other party in writing in advance. If that is not possible, confirm the intention to record the other party at the start of the recording. The organizer can remind the other participants at the outset of the meeting that it is being recorded. Any software functions that notify virtual meeting participants of a recording in progress should not be turned off or circumvented in any way. The organizer should also decide to withhold granting or otherwise permitting access to controls over the recording and transcription functions of the virtual meeting software to any other participant.

The transcriptions and recordings provide an accurate record of discussions that can be revisited to clarify details of the meeting.

5. Prohibited uses

Virtual meetings may also include AI-enabled features that may involve sensitive biometric data. These additional features should only be used to support legitimate business needs.

An organization can restrict the use of AI-enabled features in its virtual meeting policy. For example, organizations can state in their policies that use of facial recognition or sentiment/emotion analysis is prohibited unless expressly pre-approved.

Further, the organization can stipulate that AI-enabled virtual meeting tools should not be used to:

- Monitor individuals covertly.
- Analyze or evaluate individuals' emotions or productivity without consent.
- Store or process sensitive data on platforms that are not approved.
- Record or transcribe meetings without proper notification.
- Replace the proper and satisfactory performance of duties (for instance, ensuring accuracy of any meeting transcription).
- Engage in any illegal activities, unethical or harmful behaviour, or conduct in violation of any of the organization's policies.

Ensure the meeting tools do not unfairly discriminate against individuals based on protected grounds.

6. Personal information

Recordings and transcripts can contain personal information (meaning any information relating to a living individual who can be identified from that information, which can be factual such as for example, a name, address or date of birth or it can be an expression of opinion about that person, his or her actions and/or behaviour, or as such term is defined in any applicable privacy legislation) and other sensitive data (information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, or sexual life, genetic and biometric data).

A company should only collect and use personal information for specific, legitimate purposes. Avoid secondary use without additional consent. No such information shall be used or distributed except in accordance with any applicable law and the organization's policies.

A company should inform employees about the recording and transcription of meetings, specifying how the data will be used and who will have access. Ensure that only necessary information is recorded and transcribed. Avoid capturing side conversations or irrelevant data.

As a best practice, if a meeting (e.g., a virtual meeting discussing the health condition of an employee with human resources) will involve sensitive information (e.g., personal identifiable information, or biometric data) about one or more of the participants then the consent should be obtained from the relevant participants before recording and transcribing the meeting.

Any disclosure of personal information collected through the recording, transcription or summary of a virtual meeting should also be reasonable and proportionate. Organizations should consider who should have access to recordings, transcripts, and summaries. Store recordings and transcripts securely, with restricted access to authorized personnel only. If files are to be widely

circulated (or posted on an internal platform where everyone can access them), this should be conveyed to all meeting participants.

Personal information collected through recordings and transcripts must be processed fairly and lawfully, only for the limited purposes for which such data was collected. The content of the recordings and transcripts shall not be used for any activity that contravenes these principles, including unlawful monitoring or discriminatory decision-making. Be mindful of employees' rights to access, correct, and withdraw consent for their personal data.

A company should have a breach response plan in place to respond to any unauthorized disclosure or breach of recordings or transcripts, including notification procedures and mitigation steps.

7. Confidentiality and intellectual property

Recordings and transcripts can contain confidential information and intellectual property (IP). Meeting recordings provide valuable evidence of what IP was shared during the meeting, and by whom. The recording itself may be protected by copyright depending on the context. Marking the recording with a copyright notice can deter unauthorized use and distribution. If the recording contains confidential information (such as patentable subject matter), clearly mark recordings and related documents as “Confidential.”

A meeting organizer can provide notice to meeting participants not to share or display work unless necessary permissions have been obtained or an exception applies. This can be done by displaying or reading a notice at the start of the meeting. The organizer can remind presenters of the importance of only sharing original or properly licensed content. Users should not incorporate or share third-party intellectual property into a virtual meeting unless the users have prior authorization from such third party. Attendees should be encouraged to use materials that are original, in the public domain, or covered by open licenses, instead of using third-party works without permission. If a recording contains infringing material, a company can remove or edit the recording if possible.

Attendees should avoid disclosing any company confidential information or sensitive IP during a meeting that involves participants from other organizations. If required for the meeting, a participant sharing sensitive material during the meeting should obtain approval in advance and confirm that the meeting is confidential and the other participants are obligated to keep the contents of the meeting confidential before sharing any company confidential information. Any confidential information and IP shared during meetings should be clearly labelled or otherwise identified and ensure participants understand its sensitivity and restrictions on use. Adding copyright and confidentiality notices to the shared content may help prevent misuse. Confidentiality agreements can formalize the expectation of privacy and confidentiality among meeting participants. Users making, using or sharing the recording or transcript should comply with any requirements applicable to confidential information captured in the meeting recordings and transcripts.

Sharing and distribution of recordings should be limited to only those that require it for legitimate business purposes. A company should refrain from distributing or copying the recordings or transcripts without reviewing the material to proactively identify potential issues (such as confidential information and copyright works) and confirm permissions. The meeting recording is a helpful record that can be reviewed to identify the different works, and the associated contributors and authors. Users should avoid distributing or copying the recordings or transcripts (and the intellectual property contained therein) to anyone outside the organization unless they confirm that they have permission from the organization to do so.

When multiple parties are involved in meetings, the host of meeting can inform participants about expectations regarding the ownership, confidentiality and usage of recordings and transcripts. Advanced notice to participants helps establish an agreement and clarify any rights associated with participants' contributions. A meeting notice can indicate that by participating in the meeting and presenting original works (e.g., slides, documents) then participants permit to the making, sharing or copying the recording. The meeting notice can inform all participants that the meeting will be recorded, and whether the meeting should be considered confidential or not confidential.

Participants can be reminded of confidentiality obligations, especially if sensitive or proprietary information will be discussed. Material shared during the meeting can be clearly attributed to specific individuals during the meeting so that other participants are aware of the source of those meeting contributions. Key contributions and decisions can be summarized at the end of the meeting for the record. Respect moral rights by ensuring authors are credited and their works are not used in a derogatory manner. If possible, confirm in writing the ownership of any IP generated during the meeting, and have participants sign IP assignment or confidentiality agreements before the meeting.

Meeting recordings can be reviewed to help establish authorship, inventorship, agreements about the protection of confidential information and permitted usage of IP shared during the meeting. If participants agree to assign rights, maintain confidentiality, or otherwise manage IP during a meeting, the recording can serve as evidence of these agreements. This is especially useful if written documentation is lacking or ambiguous. However, it is best practice to follow up the meeting with written document confirming the rights or other permissions granted during the meeting particularly if the recordings capture important IP.

8. Secure storage and access

Organizations should store the recordings and transcripts securely and ensure they are accessible to authorized personnel only.

Access to recordings and transcripts can be strictly limited to those who have a clear business need to consult them for the purposes for which they were created. Meetings should be conducted in secure environments to prevent unauthorized access. Any individual responsible for storing or handling recordings and transcripts must maintain appropriate technical and organizational measures to safeguard against unauthorized access, accidental alteration, or unlawful disclosure. Organizers should ensure their own set of data is logically or physically separated from other organizations, especially when using shared infrastructure or multi-tenant cloud environments. This helps maintain confidentiality and integrity, particularly when sensitive or regulated data is involved. Safeguarding measures may include access controls such as password protection, secure file-sharing systems, and encryption, as well as administrative controls like usage logs and internal audit trails.

When using third-party service providers, organizations remain accountable for the personal information processed on their behalf. This means organizations must conduct due diligence, enter into binding agreements that specify privacy and security obligations, and monitor compliance with these requirements. Service providers should be contractually obligated to use the data only for authorized purposes, to implement appropriate safeguards, to notify organizations of any breach of the information they are handling on their behalf, and to destroy the information after the end of the agreement.

A company should define (and document) retention periods for recordings and transcripts. Such material shall only be retained for as long as is necessary to fulfil the specific purpose for which it was collected, after which it will be securely deleted. Where relevant legal or regulatory

obligations mandate a longer retention period, the content can be safeguarded under heightened security protocols until the obligation ceases to apply, after which the records will be securely deleted. Implementing a retention policy and ensuring data is destroyed as required under it can lessen the organization's risk that any commercially sensitive data, personal information, or confidential data becomes subject to a confidentiality incident. Participants who believe their personal data has been stored unlawfully or longer than required may raise any questions or concerns in accordance with the organization's data subject rights procedures. Users should ensure any sensitive information shared during the meeting is handled in accordance with the organization's data protection policies.

It is also important for the organization to have incident response plans in place to ensure data is handled responsibly throughout its lifecycle and have implemented proactive risk mitigation strategies. For example, organizations can minimize the storage of sensitive data, such as video or audio recordings, by deleting them as soon as they are no longer needed and retaining only the necessary transcripts or summaries. This reduces the potential impact of a confidentiality incident. Many privacy laws in Canada require organizations to report certain breaches to regulators and affected individuals and maintain a record of all confidentiality incidents.

9. Attending meetings of other organizations

An organization may require that employees obtain prior permission from the organization before participating in a meeting organized by a third party that will be recorded or transcribed.

An organization can stipulate that users must refrain from disclosing confidential information, intellectual property of the organization and any other sensitive data (including personal information) in the virtual meeting organized by another party. Users should request a copy of the recording and/or transcription from the third party to review and confirm that no confidential information or intellectual property of the organization in the virtual meeting, and any other sensitive data (including personal information) was recorded or captured in the transcript.

Appendix A: Internal policy template

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com