PRIVACY COMMISSIONER RELEASES MORE GUIDANCE FOR VIDEO TELECONFERENCING COMPANIES

Posted on November 3, 2021

Categories: Insights, Publications

In July 2020, the Office of the Privacy Commissioner of Canada (the "**OPC**"), along with its international counterparts, sent a letter to five of the largest video teleconferencing companies ("**VTCs**") inviting them to discuss how they address key privacy risks associated with video teleconferencing.

Based on the responses from some of the VTCs, the OPC recently shared some good practices and areas for improvement within the video teleconferencing industry.

Security

The OPC endorsed VTCs adopting a mix of vulnerability testing measures, including:

- "bug bounty" programs, through which VTCs would compensate users who identify and report security exploits;
- independent audits of VTCs' privacy and security measures; and
- simulated cyber-attacks.

VTCs are also encouraged to implement pre-employment checks (subject to applicable employment and privacy laws), regular employee training programs, and vetting and auditing procedures for third party data processors to ensure compliance with applicable data protection obligations.

Privacy-by-Design and Default

VTCs are encouraged not to treat privacy as an afterthought, and instead to proactively consider the privacy implications of new features. The OPC also recommended making standard user settings the most privacy-protecting options, for example by configuring meeting passwords and waiting rooms to be automatically enabled, and cameras and microphones to be disabled, by default.

Know Your Audience

Recognizing the increased use of video teleconferencing in privacy-sensitive contexts such as education and healthcare, the OPC has highlighted industry-specific best practices such as teacher-controlled access to

school meetings and secure screen sharing of health documents.

The OPC also recommends that VTCs create tailored guidance about the privacy features of their platforms for specific groups of users and use cases, to help individuals select the privacy settings and features most appropriate for them.

Transparency

The OPC endorses a layered approach to alerting users to the collection and use of their personal information, including through the use of notifications both before and during a video call.

The OPC has also stressed the importance of transparency when users' information is shared with third parties and requires that users be notified about what is shared, with whom it is shared and the reasons for doing so. Strategies in this respect could include up-to-date privacy notices setting out this information, as well as advance notification periods for the use of new third party processors.

End-User Control

The OPC recommends the implementation of several features to allow end users to exert control over the collection and use of their personal information, including allowing users to enable virtual and blurred backgrounds, requiring an individual's consent prior to a host activating their microphone or webcam, and the inclusion of tools for users to report inappropriate conduct during a video call.

Encryption

The OPC recommends that VTCs:

- make end-to-end encryption an option for all users;
- clearly communicate the differences between end-to-end and standard encryption;
- clearly present meeting controls that allow users to select and see the type of encryption used in a meeting; and
- enable end-to-end encryption by default in privacy-sensitive contexts such as tele-health.

Secondary Uses of Personal Information

Where personal information is used for purposes other than to provide functionality to the features of a video teleconferencing service, the OPC recommends that VTCs make this clear with plain language, direct and proactive messaging, explaining what personal information will be used for secondary purposes and why.

If these secondary purposes include targeted advertising or tracking, the OPC recommends that VTCs only engage in such practices if users have opted-in.

Storage of Personal Information

The OPC recommends that VTCs clearly communicate to users where their personal information will be stored and, where possible, give users choice over where their personal information is stored. In any event, VTCs should take appropriate steps to ensure that personal information is adequately protected wherever it is stored.

Implications for Businesses

The implications for VTCs are clear: consider implementing these recommendations of the OPC or risk adverse findings in the event of a privacy complaint or investigation initiated by the OPC.

However, many of the points raised by the OPC in this guidance echo existing statutory obligations, regulatory guidance and/or past investigation findings by the OPC which apply to a wide variety of organizations who collect, use or disclose personal information in the course of their commercial activities. This guidance therefore serves as a good reminder to consider privacy law implications early in the design phase of a new product or service and to be vigilant for ways to improve privacy and data protection practices throughout the lifecycle of that product or service.

Moreover, organizations governed by Canadian privacy laws should keep in mind that they are generally accountable for the processing of personal information by their service providers. This includes conducting appropriate due diligence to assess vendors' data handling practices and compliance with Canadian privacy laws. Organizations are advised to carefully consider the privacy practices and features of any video teleconferencing platforms used, including the points raised by the OPC in this guidance. Implementing appropriate policies and training for employees who use video teleconferencing platforms to perform their duties is also recommended to prevent data breaches and other privacy mishaps.

by Kristen Pennington, Kamal Azmy (Articling Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.