Torkin Manes
Barristers & Solicitors

Article

Technology, Privacy & Data Management

July 2020

No Free Lunch: Global Privacy Regulators Set Expectations of Video Teleconference Providers

VTC companies should make data protection and privacy integral to their services

By Lisa R. Lifshitz

While the availability of videoconferencing technology has been a salvation for many given the challenges of working remotely during the COVID-19 pandemic, the use of such technology is not without privacy and security risks.

Some users have fallen victim to so-called Zoombombing or Zoom raiding incidents in which their business meetings were hijacked by internet trolls and hackers who inserted racist, anti-Semitic, sexist and profane imagery on their screens and chat boxes, or otherwise disrupted their audio feeds. Many videoconference platform providers were seemingly caught unawares, scrambling to shore up their security settings by hastily releasing updates in order to patch critical vulnerabilities and convince users that they could continue online collaboration safely without fear of unwanted intruders.

Global privacy regulators have taken notice of the headlines (and spectacular stories) involving security flaws and in response, on July 21, the Office of the Privacy Commissioner of Canada along with five other data protection and privacy authorities – the U.K. Information Commissioner's Office, the Office of the Australian Information Commissioner, the Gibraltar Regulatory Authority, the Office of the Privacy Commissioner for Personal Data, Hong Kong, China, and the Federal Data Protection and Information Commissioner of Switzerland ("Privacy Regulators") – published an open letter to companies offering video teleconferencing ("VTC"), reminding them of their legal obligations to handle personal information responsibly. The Letter is intended for all companies that offer video conferencing services, and has also been sent to Microsoft, Cisco, Zoom, House Party and Google.

The Letter states that its purpose is to set out the Privacy Regulators' concerns and clarify the steps they should be taking as VTC companies to mitigate the identified risks and ultimately "ensure that our citizens' personal information is safeguarded in line with public expectations and protected from any harm." It then

proceeds to provide a non-exhaustive list of the data protection and privacy issues associated with VTC services. The Letter identifies key principles that should guide VTC companies, as set out below.

Security: Not surprisingly, security is listed as the Privacy Regulators' premier concern. Security is a "dynamic responsibility," and security vigilance by VTC organizations is paramount. The Privacy Regulators acknowledged the worrying reports of security flaws in the VTC products leading to unauthorized access to accounts, shared files and calls, and called for minimum standard safeguards to be deployed, including effective end-to-end encryption for all data communicated, two-factor authentication and strong passwords. This will be especially important for VTC platforms in certain sectors that routinely process sensitive information, such as hospitals providing remote medical consultations and online therapists, or where the VTC service allows sharing of files and other media, in addition to the audio-video feed.

The Privacy Regulators also expect VTC providers to stay current, remain aware of new security risks and threats to their VTC platforms, and "be agile in your response to them." Users of the platforms should be routinely required to upgrade the version of the app they have installed, to ensure that they are up-to-date with the latest patches and security upgrades. Additionally, all information must be adequately protected when processed by third parties, including in other countries.

Privacy-by-design and default: Consistent with the Canadian privacy-by-design approach to data protection and security, the Privacy Regulators note that data protection and privacy should be "baked into" VTC services. If they are mere afterthoughts in the design of a VTC platform, then there is a greater likelihood of failure that leads to "well-documented accounts of unexpected third-party intrusion to calls."

Accordingly, VTC companies should be taking a privacy-by-design approach to VTC platforms, making data protection and privacy integral to the services provided to customers. Practically, this means that the most privacy-friendly settings should be default (similar to the principle of least privilege in cybersecurity). Settings should be prominent and easy to use, including implementing strong access controls as default, clearly announcing new callers, and setting their video/audio feeds as mute on entry; applying features that allow business users to comply with their own privacy obligations, including features that enable them to seek other users' consent; and minimizing personal information or data captured, used and disclosed by the product to only that information necessary to provide the service. Additionally, VTC providers should undertake privacy impact assessments to identify the impact of their personal information handling practices on the privacy of individuals, and implement strategies to manage, minimize or eliminate these risks.

Know your audience: The Privacy Regulators acknowledged that during the COVID-19 pandemic many of the VTC platforms were being used in ways for which they were not originally designed, creating unanticipated risks. Therefore VTC companies should now be reviewing the new and different environments and users of their platforms, in order to better understand and identify children, vulnerable groups, and contexts where discussions on calls are likely to be especially sensitive (in education and health care, for example), or when operating in jurisdictions where human rights and civil liberty issues might create additional risk to individuals engaging with the VTC services. As a follow-up step, VTC companies should assess the necessary data protection and privacy and requirements for all contexts in which their platforms are now being used, and implement appropriate measures and safeguards accordingly.

Transparency and fairness: As a result of several high-profile privacy breaches over recent years, the Privacy Regulators note that global audiences now have a heightened awareness (and expectations) regarding how companies should appropriately handle their personal information and use their data. VTC companies that fail to tell their customers how they use their information, or use the information unfairly or unreasonably, may therefore not only be in violation of the law but may forfeit the trust of their users as well.

Accordingly, providers of VTC services should be upfront about what information they collect, how they use it, who they share it with (including processors in other countries), and why. This is particularly relevant should the VTC do something with the user data that is not expected because it would not be seen as a core purpose of the VTC service. Such disclosure should be provided pro-actively, be easily accessible and not simply buried in a privacy policy. Where express user consent regarding the handling of personal information is required, VTC providers should also ensure that such consent is specific and

informed. As well, VTC providers should assess the impact any future changes to the VTC platforms will have, and whether users be made aware of these changes in order to ensure users can make informed decisions about how they use the platform going forward.

End-user control: While end-users may often have little choice about the particular use of a VTC platform if their organization has already chosen to use or purchase a certain service, users should be aware that some features of particular VTC platforms may raise the risk of covert or unexpected monitoring and should be better informed (and have more control) over these processes.

For example, users must understand if VTC platform allows the host to collect their location data, track their engagement or the attention of participants generally, or record or create transcripts of calls. Ideally this is communicated to users through icons, popups or other measures (and not buried in the fine print of the platform's terms of service). Where possible, VTC companies should also include a mechanism for end-users to choose not to share that information, i.e. via opt-out, noting that opt-in mechanisms might be more appropriate in certain instances.

Conclusion: While it is clear that the Privacy Regulators recognize the value and importance of the services offered by the VTC companies during the COVID-19 pandemic, the Letter reiterates that such solutions must not come at the expense of people's data protection and privacy rights. Focusing on the key areas identified in the Letter will help VTC companies not only comply with applicable data protection and privacy laws but help build the trust and confidence of their customers and user base. The Privacy Regulators concluded the Letter by welcoming responses from VTC companies by Sept. 30, 2020, asking them to demonstrate how they are taking these principles into account in the design and delivery of their services. Responses will be shared amongst the joint signatories to this letter, though it remains to be seen whether VTC providers will take up the challenge posed by the Privacy Regulators.

This article originally appeared in Canadian Lawyer.

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner of the firm in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the past president of the Canadian IT Law Association.