mcmillan

Privacy Law Bulletin

July 29, 2020

Global Privacy Authorities Remind Video Teleconferencing Companies of Privacy Expectations

On July 21, 2020, the Office of the Privacy Commissioner of Canada (the "**OPC**") published a letter, along with privacy authorities from across the globe, to remind video teleconferencing ("**VTC**") companies of their obligations regarding user's privacy.[1] Their goal is to provide companies with principles which can help them identify and address privacy risks and better protect the personal information of users. As stated in the letter, "the ease of staying in touch must not come at the expense of people's data protection and privacy rights."

VTC services have experienced a massive surge in demand during the COVID-19 pandemic, with a record 62 million downloads during the week of March 14th.[2] This was an increase of 90% from the average downloads in the previous year, and is being seen across several popular VTC services.[3] Uses range from education or work-relation to social purposes, all of which pose particular privacy concerns.

---

[1] Office of the Privacy Commissioner of Canada. *Joint statement on global privacy expectations of Video Teleconferencing companies*

[2] "COVID-19 Outbreak: Video Conferencing Demand Rises due to Social-Distancing" (7 May 2020) online: *Businesswire*

[3] Lexi Sydow, "Video Conferencing Apps Surge from Coronavirus Impact" (30 March 2020) online: *App Annie*

Zoom faced significant media attention following the rise of "Zoom bombers" – uninvited individuals who would interrupt calls.[4] In March, the FBI warned schools against the risk of online classroom hijacking following a number of reports of VTC services being interrupted by inappropriate content.[5] The OPC shared a number of guidelines for users to protect their privacy while using VTC services, but are now turning to the VTC companies themselves to protect the privacy of their users.[6]

The letter sets out a non-exhaustive list of data protection and privacy principles to guide the actions taken by VTC companies to safeguard private information and mitigate risks:

1. Security

With the increasing use of VTC and evolving state of cyber-security threats, data security is a principal responsibly of any VTC company. Increasing reports of security flaws which have led to unauthorized access to accounts, shared files and calls create a worrying trend. Security measures such as end-to-end encryption, two-factor authentication and passwords should be give additional consideration, and regular upgrades should be provided to address new security risks. This is particularly true where information is being processed by third parties and across international borders.

2. Privacy-by-design and default

Privacy should be more than an afterthought – it should be an integral portion of the VTC service design. The most privacy-friendly settings, such as strong access controls and clearly announcing new callers, should be adopted as the default settings. This also includes minimising the personal information captured, used and disclosed to only the data necessary to provide the service.

---

[4] Kate O'Flaherty, "Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat" (27 March 2020) online: *Forbes*

[5] FBI Boston, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic* (30 March 2020), online: *Federal Bureau of Investigation*

[6] OPC Blogger, "Privacy Tech-Know blog: Videoconferencing – Maintain your physical distance, but keep your personal information close" (1 May 2020), online: *Office of the Privacy Commissioner of Canada*

3. Know your audience

The rising use of VTC services amid the COVID-19 pandemic has led to VTC being used outside of the context they were designed for. VTC companies should consider how they are currently being used and what new risks this involves, such as in healthcare and education.

4. Transparency and fairness

There is a heightened awareness of how companies handle personal information, and increasing expectations regarding use and disclosure. VTC companies should be honest with what information is collected and how it is being used. They should also ensure users are aware of any changes to the platform which may impact their privacy. This information should be easily accessible and consent is informed where it is required.

5. End-user control

VTC companies should be aware that end users may have little choice about the VTC services they are using, such as in their school or workplace. The service may allow for host capabilities such as collecting location data and creating transcripts of calls. VTC companies should ensure that end users should have appropriate information and control, and provide them the same level of honest communication and transparency they do with the host.

These principles are intended to not only ensure compliance with data protection and privacy laws, but also built trust and confidence of VTC users. The letter also reminds VTC companies that they are expected to consult with privacy regulators regarding any risks or issues which arise. In addition, they are welcoming responses from VTC companies to demonstrate how they are applying these principles to their design and delivery. It is unclear if these responses will be made available to the public.

If you have any questions relating to your privacy program or use of VTCs, please do not hesitate to contact a member of our Privacy and Data Protection Group.

by Grace Shaw and Kristen Shaw (Summer Student)

For more information on this topic, please contact:

Vancouver	Grace Shaw	236.826.3064	grace.shaw@mcmillan.ca

a cautionary note