CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY & NFP LAW BULLETIN NO. 505

NOVEMBER 25, 2021

EDITOR: TERRANCE S. CARTER
ASSISTANT EDITORS: NANCY E. CLARIDGE,
RYAN M. PRENDERGAST AND ADRIEL N. CLAYTON

OPC JOINS INT'L PRIVACY AUTHORITIES TO PROMOTE THE PROTECTION OF DATA IN VIDEO-TELECONFERENCING SERVICES

By Esther Shainblum and Martin U. Wissmath[*]

A. INTRODUCTION

CANADA'S PRIVACY COMMISSIONER joined several other countries to engage global leading companies providing video-teleconferencing technology ("VTC") in an effort to mitigate privacy risks and ensure best practices to protect personal information. The Office of the Privacy Commissioner of Canada joined privacy authorities from Australia, the United Kingdom, Hong Kong [SAR, China], Gibraltar and Switzerland (the "Authorities") in a July 21, 2020 joint statement[1] inviting five of the world's largest VTC companies to reply, leading to an October 27, 2021 announcement and report, "Observations following the joint statement on global privacy expectations of video teleconferencing companies".[2] Microsoft, Google, Cisco and Zoom responded (the "Companies") — Houseparty, another social networking service that allowed group video chatting, did not respond, but ceased operations in September 2021.

The Authorities addressed privacy issues involving the general use of large public VTC platforms, rather than focusing on specific contexts such as telehealth or education where sensitive information is shared. The joint statement noted the Companies' "responsibility for protecting the privacy rights of citizens of

[*] Esther Shainblum, BA, LLB, LLM, CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office. Martin U. Wissmath, BA, JD, is an associate at Carters practising in the areas of IT and business law.

[1] "Joint Statement on global privacy expectations of Video Teleconferencing companies", *Office of the Privacy Commissioner of Canada* (21 July 2020) ["Joint Statement"], online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/let_vc_200721/.

[2] *Office of the Privacy Commissioner of Canada* (27 October 2021) ["Report"], online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/vtc_211027/.

the world" and acknowledged the "sharp increase in the use of VTC for both social and business purposes" as a result of the COVID-19 pandemic.[3] The Authorities highlighted their concerns about whether "privacy safeguards were keeping pace with the rapid increase in the use of VTC services during the global pandemic", and provided "guiding principles to address key privacy risks."[4] The report outlines five principles or "good practices" and offers three additional recommendations for further improvement, summarized in this *Bulletin* below.

B. PRIVACY 'GOOD PRACTICES' PRINCIPLES[5]

FIVE privacy principles were identified to address key privacy risks in the Companies' services.

1. Security

   a) Regular testing of security measures. The Companies reported taking various approaches, including "penetration tests; threat modelling; 'bug bounty' programs; independent audits; internationally recognised certification; and the use of open source code to enable third party scrutiny." The Authorities recommended that VTC providers take a comprehensive and layered approach to testing of security measures.

   b) Ensuring employees and third parties understand and comply with their obligations around access to, and handling, of personal information. The Companies reported having practices in place, such as pre-employment checks, regular employee training, vetting and audits of third parties and limiting employee access "to that required for their job functions."

2. Privacy-by-design and default

   a) Data protection and privacy must be embedded into services, and not simply an afterthought. The Companies reported having detailed privacy programs in place or under development, including privacy impact assessments and "adherence to the data minimisation principle". The Authorities recommend that all VTC companies should adopt an overarching privacy program for their organisation.

[3] Joint Statement, *supra* note 1.
[4] Report, *supra* note 2.
[5] All quotations in this section and section C, *below*, are from the Report, *ibid*.

b) The Authorities recommended that the default settings for all VTC services be placed "at the most privacy protective" such as requiring passwords, waiting rooms, turning off video and muting microphones by default.

3. Know your audience

a) Companies must ensure enhanced features for particularly sensitive contexts, such as healthcare and education. This can include teacher-controlled access and secure screen sharing.

b) Guidance tailored to specific groups using VTC services is a good practice and the Companies reported examples of custom-guidance, such as documentation for teachers, advice for parents or video tutorials for entrepreneurs.

4. Transparency

a) Layered notices are a good approach to informing people how their information is collected and used, which is a "key tenet of data protection and privacy regimes worldwide." Examples include detailed notices "delineating different categories of personal information collected; privacy check-up features" and "pop-up written or audible notifications during calls", letting people know that data is being collected through recording or transcripts.

b) Users of VTC services must be informed about any personal information shared with third parties: who those third parties are and why that information is shared. Examples of good practice in the report included identifying contractors and reasons for processing information; 6-month notice before using a new third-party processor; and publishing transparency reports regarding law enforcement or government uses of data.

5. End-user control

a) "Meeting controls": Users of VTC services must be given "intuitive and clear controls" and alerted to any information about them that is collected. Good practice examples included the ability to opt out of attendance or engagement reports; virtual and blurred backgrounds; user consent prior to having the host unmute audio or activate video; and the ability to report users for inappropriate conduct.

b) "Risk management": Companies should mitigate the risks of VTC users unknowingly jeopardizing the security and privacy of meeting participants by publicizing meeting

information, such as on social media. Companies noted some innovative examples including using a tool to scan media and to alert meeting hosts of at-risk meetings, encouraging them to secure the meeting or schedule a new one.

C. RECOMMENDATIONS FOR IMPROVEMENT

THE REPORT listed three additional recommendations "to further enhance or improve some of the measures reported".

1. Encryption

   - Companies should make "end-to-end encryption" (which encrypts data at the sender's end and decrypts it at the receiver's end so that it's decrypted after arriving on the receiver's device) available to all VTC users

   - Clear and easily understandable information should be provided to users about the limitations of "standard" encryption vs. end-to-end

     - Meeting participants should be able to easily see the type of encryption being used

   - In sensitive settings, such as tele-health, end-to-end encryption should be set by default

2. Secondary use of data

   - VTC services should only use information in ways that users would "reasonably expect" and not retain information longer than necessary to operate the service

   - Where personal information is used for "secondary purposes", Companies should "explicitly make this clear to users with proactive, upfront and easily understandable messaging about what information is used and for which purposes"

     - Companies should not employ targeted advertising or the use of tracking cookies unless users have expressly opted-in to such processing

3. Data centres

   - VTC providers should be fully transparent with users on the locations where data is stored and through which it is routed

- Where possible, users should have the choice to decide which locations and jurisdictions their personal information is stored in and routed through

- Measures should be implemented, such as by contract, to ensure information is adequately protected when shared with third parties, including in foreign jurisdictions[6]

D. CONCLUSION

RECOGNIZING that dependence and general use of VTC services is likely to continue through the pandemic and beyond, the report noted how "[h]igh standards, robust measures, and best practices for privacy and security in the VTC industry for the safe deployment of these services and the ongoing trust of business and personal users". The Authorities stated their commitment to "continue to make themselves available to all VTC companies for any further engagement to support the maintenance and development of their services in a privacy protective, safe and trustworthy manner."[7]

Charities and not for profits utilizing VTC services should be aware of the risks associated with these services and should put in place their own measures — such as employee training on the safe use of VTC — to mitigate these risks.

[6] See Esther Shainblum, "Outsourcing and Transfers of Personal Information for Charities and NFPs", *Spring 2021 Charity & NFP Webinar Series* (25 May 2021), online: *Carters Professional Corporation* <https://carters.ca/pub/webinar/2021/spring-cnfp/Outsourcing-and-Transfers-of-Personal-Information-for-Charities-and-NFPs-May-25-2021.pdf>.
[7] Report, *supra* note 2.