Yukon
Information
and Privacy
Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

APPLICATIONS TO HELP YOU WORK FROM HOME

Know the risks, avoid the risks

April 8, 2020

As a result of the COVID-19 pandemic, many Yukoners are now working from home. In many cases, they are using applications developed to accommodate digital socializing and remote work through such tools as file sharing, collaborative file editing, teleconferencing and chat. There are privacy risks associated with some of these applications that Yukoners should be aware of, in order to stay cyber-safe during this global crisis.

Working remotely is not new. Many jobs provide the opportunity to work partially from home or another remote location. In the last decade, the choice of applications to support remote work has grown significantly. The most recent additions to a long list of popular applications used to work, teach, socialize and interact remotely include Zoom, Slack and Houseparty. Older applications include cloud storage and cooperation solutions such as Skype for Business, Google Drive, OneDrive, Dropbox, and iCloud. There are also messaging and video conferencing capabilities through WhatsApp and Facebook Messenger.

Enabling remote work in a responsible way

The most important thing to remember when selecting an application for remote work is to use only applications that have been approved by your workplace. If you are a manager in your workplace, it is your obligation to ensure your employees know what applications are available to them and make sure that these applications will not violate privacy laws[1] and will comply with corporate and legal security requirements.

[1] Depending on the sector you work in, see the *Access to Information and Protection of Privacy Act* (ATIPP), the *Health Information and Privacy Management Act* (HIPMA), which are both Yukon laws, or the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which is federal legislation.

Before using an application for remote work, ask your IT department or IT provider if they have vetted the application for security.[2] If you have a designated privacy officer, ask if that person has vetted the application for privacy law compliance.

Even with proper technology and policies in place, training is still necessary to inform employees of the risks associated with using these applications and to teach them how to use the applications responsibly. Your organization has work to do if your employees do not know the answers to questions such as:

- Can I share documents via the chat application we use?
- Can I record a video meeting as a transcript?
- Can I use chat to make decisions about a case file?
- Can I use the same password for a remote work application as for my corporate account?

Using video conferencing: the risks

Video conferencing applications carry some inherent risks not dependent on the specific technology used. Broadcast video can be recorded by anyone taking part in the conversations. Sometimes recording is native to the application in use but, if not, a smartphone camera can be used to achieve the same effect. Someone's image is their personal information and is protected by law. If some or all of a video conference is recorded or shared, privacy laws must be complied with.[3]

Data integrity must also be protected under privacy laws and may be at risk if a recorded video is altered. Videos are susceptible to alterations that appear very realistic, with the rise of deep-fake technology.[4]

Using chat: the risks

Remote workers may be using chat applications that are designed to message (such as texting, WhatsApp, etc) or chat functions incorporated within video conferencing applications.

A chat that is work-related is more than just a chat; it is a business record. Without proper controls in place, chat conversations may contain personal information (for example, opinions or decisions about a person) and may constitute substantive records with associated obligations to retain and protect these records. Chat functions may even be used to transfer complete documents, with all the risks of retention of these documents on intermediary servers and endpoints alike. These risks include privacy breaches, unauthorized disclosures or alterations.

---

[2] Susceptibility to exploitation and history of vulnerabilities

[3] Exceptions apply for public figures.

[4] For an example, see https://www.youtube.com/watch?v=gLoI9hAX9dw.

Mitigating the risks

An organization should give some thought to the purpose of using video conferencing and chat applications, and enforce a policy that mandates employees to act in accordance with the purpose. If sensitive information is transmitted, higher standards must be met. Security requirements for the technology may differ and should be adjusted to ensure that privacy will be protected to the highest degree possible or, at minimum, as required by privacy law.

Use of third party services: you are responsible

Remote work applications should not be used for transmitting personal information without evaluating if there are privacy or security risks associated with their use.

Public bodies in Yukon are required by the *Access to Information and Protection of Privacy Act* (ATIPP Act) to properly secure personal information against such risks as unauthorized collection, use, disclosure and access. They are also required to maintain the integrity of personal information, ensure it is accurate and prevent it from loss or unauthorized disposition. Custodians of personal health information have similar responsibilities under the *Health Information Privacy and Management Act* (HIPMA).

Public bodies are responsible if a privacy breach occurs as a result of using a third party service provider including when the service is provided via the cloud. Before acquiring or while evaluating the use of technologies that support remote work, it is strongly recommended[5] that a proper risk assessment be conducted prior to their use, including a Privacy Impact Assessment (PIA) and a Security Threat and Risk Assessment (STRA), as well as having a breach policy, procedure and training in place.

If, due to urgent circumstances, rapid implementation is required and doing a full assessment (PIA, STRA) is not feasible, a quick scan of the risks guided by the principles of the PIA and STRA will help prevent non-compliance with Yukon's privacy laws.

For more information about technology-based privacy and security threats due to COVID-19, go to https://cyber.gc.ca/en/news/staying-cyber-healthy-during-covid-19-isolation

The purpose of this document is to inform Yukoners about the risks associated with the use of videoconferencing and chat applications for personal and professional use and to support public bodies subject to the ATIPP Act and custodians subject to HIPMA in meeting their privacy and security obligations under these laws.

This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of the ATIPP Act and HIPMA, please read the Acts and regulations in their entirety. This document is not binding on Yukon's Information and Privacy Commissioner.

[5] For some custodians, PIAs are mandatory under HIPMA.