VIDÉOCONFÉRENCES : LE COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE ÉMET DES RECOMMANDATIONS

Publié le 12 novembre, 2021

Catégories: Perspectives, Publications

En juillet 2020, le Commissariat à la protection de la vie privée du Canada (le **« Commissariat »**), concurremment avec ses homologues internationaux, a adressé une lettre à cinq grandes entreprises de vidéoconférence pour les inviter à faire état de la façon dont elles s'attaquent aux risques de confidentialité.

Se fondant sur leurs réponses, le Commissariat a récemment publié quelques pratiques exemplaires et pistes d'amélioration.

Sécurité

Le Commissariat recommande aux entreprises de vidéoconférence d'adopter une combinaison de mesures d'évaluation des vulnérabilités, dont :

- des programmes de « primes à la faille détectée », soit des récompenses aux utilisateurs qui dénichent et signalent une faille de sécurité;
- la vérification indépendante des mesures de sécurité et de confidentialité;
- la tenue de cyberattaques simulées.

Les entreprises de vidéoconférence sont également encouragées à effectuer des vérifications préalables à l'embauche (sous réserve des lois applicables en matière de travail et de vie privée), à former leur personnel et à mettre en place des procédures de vérification et de validation quant aux sous-traitants qui traitent leurs données en vue de garantir leur satisfaction des obligations de protection des données qui leur incombent.

Protection de la vie privée à dessein et par défaut

Les entreprises de vidéoconférence sont invitées à réfléchir aux conséquences en matière de vie privée de nouvelles fonctionnalités dès l'étape de la conception. Le Commissariat leur recommande en outre de définir les paramètres de leurs services pour qu'ils protègent les données des utilisateurs de manière optimale par défaut, par exemple en protégeant d'office par mot de passe les salles d'attente et de réunion ou en désactivant par défaut les micros et les caméras.

Connaître son public

Reconnaissant l'essor que connaît la vidéoconférence dans des contextes particulièrement sensibles, comme l'éducation et les soins de santé, le Commissariat a recensé les pratiques exemplaires propres à ces secteurs, par exemple l'octroi aux enseignants du contrôle des accès aux réunions scolaires et la sécurisation des partages d'écran visant des documents relatifs à la santé.

Le Commissariat recommande également que les entreprises de vidéoconférence fournissent, à certains groupes d'utilisateurs ou dans des cas particuliers, des directives sur les fonctionnalités de protection de la vie privée de leurs plateformes afin d'aider les utilisateurs à choisir les configurations et fonctionnalités les plus adaptées.

Transparence

Le Commissariat recommande l'emploi d'une approche multicouche pour aviser les utilisateurs de la collecte et de l'utilisation de leurs renseignements personnels, par exemple par la transmission de notifications tant avant que pendant les appels vidéo.

Il souligne également l'importance de la transparence lorsque les renseignements d'utilisateurs sont transmis à des tiers, et exige que les utilisateurs soient avisés des renseignements qui sont communiqués et de la raison. Pour ce faire, les entreprises pourraient par exemple diffuser un avis de confidentialité actualisé faisant état de cette information ou observer un délai de préavis avant de recourir à un nouveau sous-traitant.

Contrôle exercé par l'utilisateur final

Le Commissariat recommande que les entreprises mettent en place des fonctionnalités permettant aux utilisateurs finaux de contrôler la collecte et l'utilisation de leurs renseignements personnels, notamment en leur permettant d'utiliser des arrière-plans virtuels ou flous, en rendant nécessaire le consentement à l'activation de leur micro ou caméra et en leur permettant de signaler le comportement inapproprié d'autrui lors d'un appel.

Chiffrement

Le Commissariat recommande que les entreprises de vidéoconférence :

- offrent le chiffrement de bout en bout comme option à tous les utilisateurs;
- communiquent clairement aux utilisateurs la différence entre les chiffrements « standard » et de bout en bout;
- présentent clairement les outils de contrôle des réunions permettant aux utilisateurs de voir et de changer le type de chiffrement utilisé;

- fassent du chiffrement de bout en bout le réglage par défaut dans les contextes sensibles, par exemple dans le domaine de la télésanté.

Utilisation secondaire des renseignements personnels

Si des renseignements personnels sont utilisés à d'autres fins que le fonctionnement d'un service de vidéoconférence, le Commissariat recommande que les entreprises de vidéoconférence l'indiquent par des messages directs en langage clair faisant état des renseignements personnels qui seront utilisés à des fins secondaires et des raisons derrière cette utilisation.

Si ces fins secondaires comprennent de la publicité ciblée ou l'utilisation de témoins, le Commissariat recommande que les entreprises de vidéoconférence ne se livrent à ces activités que dans la mesure où les utilisateurs y ont expressément consenti.

Conservation de renseignements personnels

Le Commissariat recommande que les entreprises de vidéoconférence indiquent clairement aux utilisateurs où leurs renseignements personnels seront conservés et, dans la mesure du possible, leur laissent choisir cet emplacement. Dans tous les cas, les entreprises devraient prendre les mesures nécessaires pour assurer la protection des renseignements personnels, où qu'ils se trouvent.

Conséquences pour les entreprises de vidéoconférence

Le message du Commissariat est clair : à défaut de donner suite à ses recommandations, les entreprises de vidéoconférence risquent de recevoir des conclusions défavorables advenant une plainte ou une enquête en matière de vie privée.

Notons toutefois que plusieurs des points soulevés par le Commissariat font écho à des obligations légales et à des orientations réglementaires en vigueur, ainsi qu'à des constats d'enquêtes passées visant diverses entités qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre d'activités commerciales. Ses instructions sont donc un bon rappel pour les entreprises de vidéoconférence de tenir compte des lois sur la protection de la vie privée dès la conception d'un nouveau produit ou service, et d'être à l'affut de pistes d'amélioration des pratiques de protection des données et de la vie privée tout au long du cycle de vie du produit ou du service.

Par ailleurs, les organisations régies par les lois canadiennes sur la protection de la vie privée devraient garder à l'esprit qu'elles sont généralement responsables du traitement que font leurs fournisseurs de services de renseignements personnels. Cela suppose qu'elles effectuent les vérifications diligentes qui s'imposent pour évaluer les pratiques de traitement des données de ces fournisseurs, de même que leur respect du droit

canadien. Les entreprises qui utilisent les plateformes de vidéoconférence ont intérêt à examiner attentivement leurs pratiques et fonctionnalités liées à la vie privée, notamment quant aux points soulevés par le Commissariat. Il leur est aussi conseillé de mettre en place des politiques et de former le personnel qui utilise ces plateformes dans le cadre de leurs fonctions afin d'éviter les fuites de données et d'autres incidents relatifs à la vie privée.

par Kristen Pennington et Kamal Azmy (stagiaire en droit)

Mise en garde