OVATION AMERICAS

Mai 2022 Infolettre

Protection de la Vie Privée, est-il déjà trop tard? (Partie 1)

Commençons-nous à payer le prix de nombreuses années d'abus de la part des grandes entreprises technologiques, du gouvernement et de nombreuses entreprises privées qui recueillent nos renseignements personnels?

Vous êtes-vous déjà demandé si nous ne serions pas réellement les victimes de nombreuses années de collecte abusive de données par pratiquement tous ceux avec qui nous avons interagi en ligne, de notre gouvernement, du secteur financier, des entreprises de technologie et, en plus de cela,

de nombreux programmes de surveillance nébuleux dans le monde entier?

Il n'y a jamais eu autant de vol d'identité, de piratage, d'activités frauduleuses telles que les ransomware, le phishing, etc. qu'aujourd'hui. Avons-nous raison de demander une meilleure protection de la vie privée? Avez-vous confiance que nos informations sont bien gérées et protégées? Dans ce bulletin mensuel, nous décidons de partager avec vous l'intégralité d'un article et d'une partie d'un autre en provenance du Canada qui illustrent bien l'état de la situation.

Le Toronto Globe and Mail opinion
Publié le 7 Mai, 2022

Qui veut vivre dans un état de surveillance? Pas les canadiens

Il serait sans doute extrêmement bouleversant pour les Canadiens de découvrir que des entreprises privées et des services de police ont recueilli sans discernement leurs empreintes digitales et leur ADN et les ont placées dans une base de données.

Et pourtant, les entreprises et les policiers ont été en mesure de le faire avec ce que l'on appelle des empreintes faciales – des données faciales biométriques aussi personnelles et immuables que

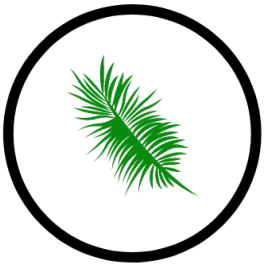
les verticilles sur un index ou le séquençage dans l'ADN – généralement sans le consentement de quiconque.

Pire encore, au Canada, la collecte et l'utilisation de la technologie de reconnaissance faciale ne sont pratiquement pas réglementées. C'est l'une des principales préoccupations soulevées cette semaine par les organismes de surveillance de la protection de la vie privée des provinces, des territoires et des gouvernements fédéraux du Canada, dans une déclaration conjointe au Comité permanent du Parlement sur l'accès à l'information, la protection de la vie privée et l'éthique.

« Contrairement à d'autres formes de données biométriques recueillies par les services de police, comme les photographies, les empreintes digitales ou les profils d'ADN, l'utilisation de la reconnaissance faciale n'est assujettie à aucune règle législative ciblée », a déclaré le commissaire fédéral à la protection de la vie privée, Daniel Therrien, au comité. « Au lieu de cela, son utilisation est réglementée par une mosaïque de lois et de jurisprudence qui, pour la plupart, ne traitent pas spécifiquement des risques posés par la reconnaissance faciale. »

C'est plus qu'inquiétant, car les risques sont énormes. Contrairement à la collecte d'empreintes digitales ou d'ADN – des processus chronophages qui nécessitent une intervention humaine – la collecte et l'analyse des données de reconnaissance faciale peuvent être complètement automatisées, grâce à l'intelligence artificielle.

Cela peut également être fait sans le consentement ou même à l'insu de la personne concernée. Ce fut le cas de Clearview AI, une société américaine qui a récupéré des sites Web de médias sociaux et d'autres sources publiques en ligne pour des photographies personnelles, et a créé une base de données de données faciales biométriques attachées aux informations d'identification de plus de trois milliards de personnes.

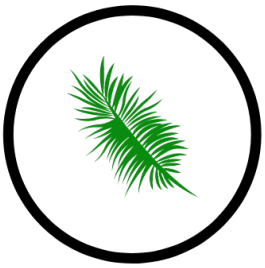


Après qu'il a été révélé que certains services de police canadiens, y compris la GRC, utilisaient les services de Clearview, le commissaire fédéral à la protection de la vie privée et trois homologues provinciaux lui ont ordonné de cesser ses activités au Canada et de supprimer les images de Canadiens de sa base de données. L'affaire Clearview est une démonstration frappante des dangers de la technologie de reconnaissance faciale. Les commissaires à la protection de la vie privée ont clairement indiqué dans leur déclaration au comité que la reconnaissance faciale peut être un outil précieux pour l'application de la loi, la sécurité nationale et la recherche de personnes disparues. Mais elle peut aussi être « extrêmement intrusive, permettre une surveillance généralisée, fournir des résultats biaisés et éroder les droits de l'homme, y compris le droit de participer librement, sans surveillance, à la vie démocratique ».

Il est facile d'imaginer comment cela pourrait être vrai. Les personnes qui participent à une manifestation publique légale ne sont pas toutes prises par la police, et leurs empreintes ne sont pas passées dans une base de données, simplement parce qu'elles se sont présentées. Evidemment non. Cela ne serait jamais permis au Canada.

Alors, pourquoi la police pourrait-elle utiliser des caméras de surveillance pour capturer les visages des manifestants, ou de n'importe qui dans un lieu public, et diffuser les images dans une base de données d'empreintes faciales? Pour beaucoup, cela dissuaderait de participer à une activité légale et démocratique. Le Parlement doit tenir compte des conseils des commissaires à la protection de la vie privée et agir rapidement pour s'assurer que les anciens droits des Canadiens ne sont pas éviscérés par les nouvelles technologies.

La loi devrait indiquer clairement quand les données faciales biométriques – tout comme les empreintes digitales et l'ADN – peuvent être collectées, auprès de qui et sous quelle autorité. L'utilisation de la technologie de reconnaissance faciale devrait être « ciblée, axée sur le renseignement et soumise à des limites de temps appropriées », ont déclaré les commissaires à la protection de la vie privée. Et le balayage de masse du visage ne devrait être autorisé que dans les circonstances les plus rares.



Il devrait également être interdit la collecte aveugle de données faciales biométriques. Il y a de bonnes raisons pour lesquelles l'État recueille les empreintes digitales des délinquants condamnés; ajouter leur empreinte faciale à une base de données aurait du sens. Mais la construction de bases de données de masse sur les empreintes faciales de Canadiens ordinaires ne peut tout simplement pas être autorisée, à des fins commerciales ou policières, dans un pays libre.

Après sept ans au pouvoir et beaucoup de discussions, le gouvernement Trudeau n'a pas réussi à adopter des lois pour freiner les big tech ou pour lutter contre le harcèlement et la désinformation en ligne. Mais ces problèmes qui font la une des

journaux font pâle figure en comparaison de la menace qui pèse sur nos libertés de surveillance de masse par la reconnaissance faciale. C'est un problème qui nous regarde en face, et il faut s'y attaquer.

True North news publié le 5 Mai, 2022

Les Canadiens devraient être informés si leurs données sont recueillies par le gouvernement fédéral : Le comité

Le comité d'éthique de la Chambre des communes veut que le gouvernement fédéral informe les Canadiens s'ils sont espionnés et leur donne la possibilité de se retirer des programmes de surveillance de la collecte de données. Ces recommandations interviennent alors que des parlementaires enquêtent sur l'Agence de la santé publique du Canada (ASPC) qui espionne secrètement les emplacements de millions de Canadiens.

L'année dernière, il a été révélé que le ministère fédéral avait obtenu des données de 33 millions d'appareils pour mener des recherches sur les « modèles de mobilité de la population » pendant les confinements. Le projet n'a été dévoilé qu'après que ASPC a publié un avis d'appel d'offres demandant aux entrepreneurs de poursuivre le programme de surveillance jusqu'au 31 mai 2023. Les membres du comité ont demandé au gouvernement d'aviser les personnes incluses dans les futurs ratissages « d'une manière qui décrit clairement la nature et le but de la collecte de données ».

De plus, les parlementaires ont déclaré qu'ils aimeraient voir des lois sur la protection de la vie privée améliorées afin de protéger les renseignements anonymisés et agrégés. En février, la Chambre des communes a voté de justesse en faveur de l'arrêt temporaire de la surveillance de l'ASPC malgré l'opposition des députés libéraux. « Nous ne sommes tout simplement pas au point de comprendre comment ces données ont été recueillies, si elles ont été correctement anonymisées, quels sont les risques de réidentification et pourquoi le commissaire à la protection de la vie privée n'a pas participé au processus », a déclaré le député conservateur John Brassard.

Le programme fait également l'objet d'une vérification par le commissaire fédéral à la protection de la vie privée. Bien que les responsables de l'ASPC soutiennent que les renseignements personnellement identifiables ont été retirés des données, les experts en protection de la vie privée ont contesté l'allégation et ont qualifié

le programme de violation des droits des Canadiens.

Ann Cavoukian, ancienne commissaire à la protection de la vie privée et directrice générale de Global Privacy and Security by Design, a déclaré à True North en décembre que les Canadiens devraient avoir « confiance zéro » dans les assurances du gouvernement fédéral concernant leur conduite. « Ils collectent toutes ces données mobiles », a-t-elle déclaré. « 33 millions d'appareils mobiles et d'appareils mobiles sont généralement liés à des identifiants personnels, et vous devez prendre des mesures pour les supprimer et désidentifier les données de manière forte afin qu'elles ne puissent pas être réidentifiées. Nous n'avons aucune assurance à cet effet. »

La protection de la vie privée et la sécurité sont vraiment une question de bonnes habitudes personnelles, mais même avec elle, il y a encore beaucoup de choses qui semblent hors de nos mains pour l'instant. Nous savons tous à quel point nos gouvernements sont doués pour gérer et sécuriser les données collectées... nos données biométriques uniques n'est-ce pas le dernier appel? Alors peut-être que c'est la raison pour laquelle nous pouvons nous demander si la situation réelle n'est pas le résultat de l'abus trop long et excessif? Les personnes mal intentionnées, obtiennent ce dont elles ont besoin en grattant facilement trop de bases de données.

Continuons à apprendre et à rester à jour sur les questions de confidentialité et de sécurité pour nous donner les meilleures chances d'éviter les piratages et les escroqueries coûteuses.

Pour des commentaires, des informations ou pour savoir comment minimiser votre exposition aux données, n'hésitez pas à nous contacter à l'adresse suivante:

info@ovationamericas.com ou visitez notre site web au: www.ovationamericas.com

OVATION
AMERICAS