TECH INFORMED POLICY

LE 18 AOÛT 2020

EXPOSÉ Nº 2 SUR UN MORATOIRE SUR LA RECONNAISSANCE FACIALE

Condition pour lever un moratoire sur l'utilisation publique de la technologie de reconnaissance faciale au Canada

Produit par

Taylor Owen, Directeur de la politique et titulaire de la Chaire Beaverbrook pour l'éthique, les médias, et la communication, Directeur du Centre pour les médias, les technologies, et la démocratie, et professeur agrégé à l'École de politiques publiques Max Bell à l'Université McGill

Derek Ruths, Directeur du Laboratoire des dynamiques des réseaux et professeur agrégé d'informatique à l'Université McGill

Stephanie Cairns, Assistante de recherche

Sara Parker, Assistante de recherche

Charlotte Reboul, Assistante de recherche

Ellen Rowe, Assistante de recherche

Sonja Solomun, Directrice de recherche, Centre pour les médias, les technologies, et la démocratie à l'Université McGill

Kate Gilbert, Graphiste

Gersande La Flèche, Traductrice

Centre *for* MEDIA, TECHNOLOGY *and* DEMOCRACY

network dynamics @mcgill
measuring and predicting large-scale human behavior

À PROPOS DE TIP

Tech Informed Policy (TIP) est une initiative lancée par deux chercheurs phares à l'Université McGill, Dr Derek Ruths, Directeur du Laboratoire des dynamiques des réseaux et professeur agrégé d'informatique, et Dr Taylor Owen, Directeur de la politique et titulaire de la Chaire Beaverbrook pour l'éthique, les médias, et la communication, Directeur du Centre pour les médias, les technologies, et la démocratie, et professeur agrégé à l'École de politiques publiques Max Bell. TIP cherche à démystifier la technologie à la base de nombreux enjeux politiques critiques et à fournir des conseils utiles et informés par cette technologie aux responsables politiques canadiens.

Nous vous invitions à contacter Derek Ruths pour nous faire parvenir vos questions ou commentaires.

Lexique terminologique

Algorithme : La suite finie de règles et d'opérations qu'un ordinateur peut suivre pour accomplir une tâche.

Base de données : Une base de données est un ou plusieurs jeux de données structurés et retenus par un système d'exploitation ou un logiciel.

Intelligence artificielle (IA) : L'intelligence artificielle est un système conçu pour accomplir une tâche qui nécessite ordinairement l'intelligence humaine. Les systèmes IA « apprennent » à exécuter des tâches en traitant des quantités énormes d'information pour reconnaître leurs formes et caractéristiques communes, et traduisent ensuite cette connaissance aux tâches.

Interface de programmation (API) : Une interface de programmation d'application fournit un cadre aux développeuses et développeurs de logiciel pour créer leurs propres applications. Elle représente une collection d'opérations potentielles que les équipes de programmation peuvent utiliser pour répondre à leurs besoins.

Jeu de donné : Un ensemble de données.

Score d'apparence (Match Score en anglais) : Une note entre 0 et 1, indiquant la probabilité qu'une paire d'images représente la même personne.

Seuil du score d'apparence (Match Score Threshold en anglais) : Une valeur entre 0 et 1, les paires d'images ayant une note au-delà de cette valeur seront identifiées comme représentant la même personne.

Vecteur de caractéristiques : Une représentation numérique des caractéristiques du visage, traitée par un algorithme IA.

SOMMAIRE EXÉCUTIF :

Cet exposé est le deuxième de deux documents sur la technologie de reconnaissance faciale (RF). Celui-ci aborde les conditions nécessaires pour lever un moratoire fédéral, tandis que le premier exposé décrit la fonctionnalité et l'utilisation de la RF, ainsi que les implications d'un moratoire fédéral.

- Ce document décrit les conditions technologiques, sociales, politiques, et juridiques nécessaires pour lever un moratoire canadien sur les systèmes de RF.
- Parmi des appels montant pour que le Canada impose un moratoire national sur la technologie de reconnaissance faciale (FR), une approche holistique aux conditions technologiques et politiques est nécessaire.[1] [2]
- Certaines sociétés privées, telles Microsoft et Amazon, ont imposé des moratoires sur la vente de la technologie de RF aux services de police, même si elles n'imposent aucune limitation sur l'utilisation actuelle de leurs services.[3] [4]4 Clearview AI a récemment cessé toute opération canadienne en raison d'une investigation par le Commissariat à la protection de la vie privée au Canada concernant l'utilisation de leurs services par la GRC et le Service de police de Toronto.[5]
- Les moratoires du secteur privé ne sont pas une solution pour répondre aux implications politiques des systèmes de RF, et ne représentent pas une solution adéquate aux problèmes structurels de la technologie. Les moratoires imposés par le secteur privé représentent plutôt une occasion pour le gouvernement canadien à établir un moratoire national sur la technologie de RF.
- Un moratoire national permettrait donc aux gouvernements un peu plus de temps pour évaluer et créer les conditions nécessaires pour une utilisation sécuritaire et équitable de la technologie par les compagnies de technologie de RF ainsi que les acteurs du secteur public.
- Ces conditions devraient inclure, entre autres : des cadres pour la gouvernance des données, des mesures de responsabilisation et pour la protection de la vie privée, et des évaluations des conséquences sociales.

    i. Les conditions technologiques pour lever un moratoire sont inséparables des considérations sociales et politiques, détaillées plus loin, et doivent toujours être implémentées en tandem pour toute décision concernant l'utilisation de la RF dans le secteur public (p. ex., si les conditions de partialité et d'exactitude sont remplies, mais pas celles de la protection des données, le moratoire ne devrait pas être levé).

ii. Pour ce faire, renforcer les lois actuelles (telle la LPRPDE, la Loi sur la protection des renseignements personnels et les documents électroniques) sera peut-être nécessaire, ainsi que la création de nouvelles politiques pour les systèmes biométriques ou spécifiques à la RF.

STRUCTURE DE L'EXPOSÉ Nº 2

CONDITIONS POUR LEVER UN MORATOIRE

Nous proposons dans ce document les conditions nécessaires pour lever un moratoire, divisées parmi les sections suivantes :

- Conditions des intentions
- Conditions d'utilisation des données
- Conditions de partialité et d'exactitude
- Conditions de revue et de supervision
- Conditions sociales
- Conditions juridiques

Dans notre discussion précédente, les préjudices causés par les systèmes de RF[6], comme l'augmentation de surveillance, la discrimination, l'utilisation abusive des données et les violations à la vie privée, ont des répercussions qui se font sentir à travers les sphères technologiques, sociales, politiques, et juridiques. Les conditions pour l'utilisation sécuritaire de la technologie doivent donc exister à l'intersection de ces domaines.

Considérations et questions

Chaque condition décrite dans ce document peut seulement être développée, formulée précisément, et finalement répondue à travers de la recherche considérable ou par la consultation avec des experts ou expertes issus des champs technologiques, des sciences sociales, de la politique, ou du droit. Certaines conditions sont claires, mais difficiles à satisfaire : la technologie de RF doit être prouvée sans préjugé avant que sa sécurité puisse être assurée, mais simplement savoir que les systèmes de RF doivent être sans biais systémique n'aide pas à réduire ou même évaluer sa présence avec certitude. D'autres conditions doivent être formulées et définies par des équipes d'experts; la technologie de RF doit adhérer à un cadre solide de gouvernance des données, mais les détails exacts de ce cadre demeurent flous.

Ces sections décrivent quelques-unes des questions et considérations principales qui doivent être adressées par les responsables politiques ainsi que par des équipes d'experts consultées avant qu'un moratoire puisse être levé.

Prochaines étapes : recherche et études pendant un moratoire

Finalement, nous décrivons la recherche, la consultation, et les évaluations qui devront être entreprises pendant un moratoire pour solidifier les conditions décrites et répondre aux questions et considérations soulevées par le processus.

CONDITIONS DES INTENTIONS

PRÉCISER L'UTILISATION DES SERVICES

Une institution publique souhaitant faire recours à un service de RF devrait préciser leurs cas d'utilisation prévus. Ces requêtes pour l'utilisation de la RF devront être approuvées par un organisme de réglementation gouvernemental et devraient spécifier :

- Le résultat souhaité (p. ex., la comparaison d'une photo provenant d'une base de donnés policière au profil du suspect saisi par la vidéosurveillance);
- Qui aura accès au service (p. ex., des hauts fonctionnaires de la police qui ont reçu une formation en RF, travaillant à partir d'une machine accessible seulement au bureau);
- Les situations dans lesquelles le système de RF sera utilisé (p. ex., l'utilisation par la GRC de la technologie de RF fournie antérieurement par Clearview AI pour la CNCEE);
- PLes cas d'utilisation qui pourront survenir un jour, mais pour lesquels l'utilisation n'est pas actuellement désignée (p. ex., la GRC testant la RF pour l'utilisation potentielle par d'autres divisions du service)

Définir l'utilisation de la RF servira à délimiter les spécifications du service de RF, les données requises, et le seuil du score d'apparence requis pour ses fonctions.

LIMITES DES INTENTIONS

L'institution devra suivre chaque cas d'utilisation actuel de la RF pour assurer que la technologie est utilisée pour atteindre ses objectifs prévus, un suivi qui sera audité régulièrement.

Considérations et questions :

Comment et par qui seront évalués les cas d'utilisation?

Les responsables politiques devront décider quelles organisations, existantes ou non, évalueront les cas d'utilisation des services de RF, et qui répondra et punira son usage impropre. Ils devront aussi déterminer qui prendra la responsabilité pour l'évaluation des cas d'utilisation interdits : un organe réglementaire indépendant ou l'institution elle-même.

Comment est-ce que les cas d'utilisation potentiels seront évalués?

Toute régulation de la RF doit inclure des provisions pour les utilisations potentielles, tout en reconnaissant qu'il est impossible de prédire ce que ressemblera l'avenir technologique, politique, et social. Cette tâche, bien que difficile, est primordiale pour assurer que toute politique post-moratoire ne traînera pas derrière les dernières innovations technologiques.

Quelles lois ou politiques doivent être mises en place pour assurer l'utilisation sécuritaire et appropriée?

Il n'est pas suffisant d'exiger que les utilisations internes de la RF suivent les lois canadiennes, puisque la loi actuelle est insuffisante pour assurer l'utilisation sécuritaire et appropriée de cette technologie. Les inspections qui cherchent seulement à vérifier que les cas d'utilisation conforment aux lois canadiennes existantes ne sont pas des conditions réalistes pour lever un moratoire.

Comment est-ce que les services de police devraient utiliser la technologie de RF? Est-ce qu'elle devrait être utilisée dans sa forme actuelle?

À cause du risque élevé d'arrestation arbitraire et de biais raciaux, l'utilisation de la technologie de RF dans son état actuel peut seulement être justifiée si elle est nécessaire pour la sécurité des Canadiens et Canadiennes.[7] [8] Par contre, des versions futures de la technologie pourraient démontrer un niveau de risque moins élevé. Un cadre de cas d'utilisation pour les forces de l'ordre devrait être équipé pour évaluer les risques ainsi que les bienfaits et déterminer quelles utilisations de la technologie de RF peuvent être permises. La mise en œuvre d'un tel cadre nécessite davantage de recherche, mais son adoption serait nécessaire pour garantir un degré raisonnable de sécurité pour l'utilisation policière de la technologie.

CONDITIONS D'UTILISATION DES DONNÉES

CONTENU DES JEUX DE DONNÉES

Tout système de RF nécessite deux collections d'images faciales : un jeu de données pour l'entraînement offert par le fournisseur du système ainsi qu'une base de données pour effectuer la recherche d'images correspondantes. Cette dernière, qui peut également contenir des noms et d'autres identifiants personnels, est créée sinon par le fournisseur (p. ex., la base de données de Clearview AI raclée à partir de l'internet) ou par l'institution utilisant le système (p. ex., les clichés anthropométrique possédées par les services de police).

Si la base de données de recherche est maintenue par le fournisseur, celui-ci devrait divulguer son contenu, son utilisation, et ses origines à l'institution qui s'en sert, ainsi que la manière dont le fournisseur récupère les données générées par leur clientèle (telles les institutions se servant du système) et le but de cette collecte.

LA GESTION DES DONNÉES

Puisqu'il s'agit de renseignements très sensibles, l'institution ainsi que le fournisseur doivent prendre toutes les précautions nécessaires et suivre les normes actuelles pour la gestion sécuritaire des données.[9] Les données devraient seulement être collectées et conservées selon la nécessité dictée par les principes de minimisation des données.[10] Les données générées par un système de RF devraient seulement être utilisées selon l'usage prévu et entreposées aussi longtemps que nécessaire, et les personnes qui figurent dans la banque d'images doivent avoir le droit de demander que leurs images soient retirées.[11] De plus, ces données doivent seulement être partagées lorsque nécessaire—incluant avec les fournisseurs.

Considérations et questions :

Quelles données pourront être saisies, en quelle quantité, et pendant combien de temps pourront-elles être conservées?

Quoique les conventions actuelles du traitement des données sont insuffisantes pour adéquatement réglementer l'utilisation de la RF, elles ne devraient pas être négligées; ces conventions devraient plutôt être étudiées, discutées, et élargies. Tout règlement futur doit équilibrer la protection des données, l'innovation de la technologie de RF, et l'environnement précis dans lequel le service est utilisé. Par exemple, les données générées par un système de RF peuvent être importantes ou même indispensables pour

la poursuite de l'amélioration de la technologie. En limitant l'accès aux données générées par la clientèle de RF, les institutions peuvent aussi limiter l'amélioration des systèmes.

De plus, il est peut-être irréaliste de s'attendre que les services de police puissent suivre les normes actuelles gouvernant les données lors de l'utilisation de la RF pour les investigations criminelles, un problème particulièrement important lorsqu'il faut déterminer la durée de temps que les données peuvent être conservées. Il est possible que seules les institutions voulant utiliser la technologie de RF puissent répondre à ces questions; cependant, ces questions nécessiteront une analyse effectuée par un organisme de gouvernance indépendant.

Est-ce que l'individu a le droit d'être informé quand la technologie de RF est utilisée sur lui?

La grande diversité d'utilisation potentielle de la technologie de RF complique l'applicabilité des conventions du consentment.[12] La technologie du RF pourrait atteindre la vie privée des Canadiens et Canadiennes, notamment à travers la collecte sans consentement des données ou l'utilisation des données par des tiers. Un environnement technologique sain qui respecte la vie privée est fondé sur la transparence, permettant à chaque utilisateur ou utilisatrice de comprendre comment leurs données sont utilisées et comment elles sont recueillies. Selon l'utilisation spécifique de la RF, sur qui la technologie sera utilisée est une question qui requiert une réponse. Est-ce que les individus seront avisés lorsqu'un système de RF est utilisé pour capturer leur image, tel dans les centres de magasinage où la vidéosurveillance est équipée d'un système de RF?[13] Est-ce que les suspects d'une investigation criminelle seront notifiées quand l'utilisation d'un système de RF a résulté dans leur arrestation? Est-ce que les données seront permises comme preuve en cour si le système de RF a été consulté sans mandat, étant donné que le sujet n'a probablement pas donné son consentement?

Est-ce que l'individu a droit au consentement quant à son inclusion dans une base de données?

Se trouver dans une banque d'image utilisée pour entraîner un système de RF présente peu de risque pour l'individu, par contre le risque est beaucoup plus important si son image se trouve dans une base de données de recherche. Certaines entreprises, comme Clearview AI, ont donné à leur clientèle la possibilité de trouver leurs sujets parmi des banques de données incluant des milliards d'images raclées de l'internet, permettant accès à n'importe quel individu avec une présence visuelle sur le web.[14] Toute proposition de cadre de gouvernance des données doit par conséquent se pencher sur comment les photos sont ajoutées aux banques de données de recherche, et si les individus ajoutés peuvent consentir à leur inclusion. Il est fort probablement impossible que chaque individu puisse être avisé quand ses images sont ajoutées à une base de données massive raclée à partir de l'internet, comme celle utilisée par Clearview AI. Exiger que les fournisseurs des systèmes de RF dénichent les coordonnées de chaque personne présente dans leurs banques d'images est non seulement infaisable, mais pourrait violer encore davantage la vie privée de la personne.

Quel principe privilégier guidera les délibérations à venir. Est-ce que les fournisseurs et les institutions ont l'obligation d'obtenir le consentement préalable? Ou est-ce qu'on devrait privilégier le droit de l'individu à demander que ses informations biométriques soient retirées des bases de données? Ces discussions devront inclure le gouvernement, les fournisseurs des systèmes de RF, et les citoyens et citoyennes canadiens.

Est-ce que les Canadiens et Canadiennes devraient avoir droit à l'oubli?[15]

Les règlements gouvernementaux doivent régir si et comment les individus peuvent retirer leurs images des bases de données, et quelles méthodes protègeront leur vie privée. Comme l'exemple récent de Clearview AI démontre, enlever son visage d'une base de données n'est pas une protection suffisante aux données biométriques. La seule manière de retirer les images d'un individu de la base de données de Clearview AI est de leur fournir une photo supplémentaire pour assurer que l'individu n'est plus jamais rajouté à la base de données.[16] Ce problème n'est pas unique à Clearview AI. Si une personne souhaite être exclue de toute base de données de recherche, elle devra fournir une photo avec—si la base de données inclut des coordonnées—plus de renseignements personnels, comme son nom. Cette information ne pourra jamais être supprimée par la suite. Une possibilité complètement anonyme, comme retenir seulement la répresentation numérique d'une photo créée par l'algorithme ne serait pas faisable, car l'algorithme continuera d'évoluer.

Puisque la démarche pour supprimer son image d'une base de données consiste d'une violation supplémentaire à la vie privée, permettre aux individus de demander que leurs images soient retirées d'une base de données ne garantit pas la protection de la vie privée.

CADRE DE GOUVERNANCE DES DONNÉES

Un cadre de gouvernance des données réglementant l'utilisation publique de la technologie devrait être mise au point, préférablement par le gouvernement. Ce cadre, axé sur la transparence et la responsabilité, devrait délimiter les conditions de l'utilisation de la RF au Canada ainsi que les meilleures pratiques des fournisseurs et utilisateurs de la technologie.[17]

L'exemple qui suit est d'un cadre de gouvernance de la RF développé par le Forum économique mondial.[18] Chacune des quatre étapes nécessite des études approfondies et beaucoup de délibération avant leur mise en œuvre.

Au centre : Meilleures pratiques pour la réalisation d'une cadre de gouvernance des données

1. Justifier le choix de la technologie de reconnaissance faciale
2. Conceptualiser un plan pour les données qui correspond avec les caractéristiques des utilisateurs et utilisatrices finaux
3. Réduire les risques de biais systémiques
4. Informer les utilisateurs et utilisatrices finaux, et être transparent

Le Règlement général sur la protection des données (RGPD) de l'Union européenne fournit un cadre responsable de gouvernance des données aux institutions et entreprises européennes, construit à partir de sept principes pour le traitement légitime des renseignements

personnels.* Considéré mondialement comme un repère phare pour la protection responsable des données, le RGPD est a été appliqué avec succès pour la première fois dans la cour française contre l'utilisation de la technologie de RF dans le secteur publique. La cour a conclu que l'utilisation de la RF au sein des écoles violent les principes de limitation des finalités du RGPD (concernant la possibilité d'accomplir le même objectif à travers une démarche moins intrusive), et la minimisation des données (concernant la collecte de données non pertinentes et excessive).[19]

LA RESPONSABILITÉ

En plus d'une gouvernance des données axée sur la RF pour les utilisations à enjeux élevés par le secteur public, des mesures (possiblement nouvelles) de responsabilisation devront être développées avant de lever un moratoire. Bien que la protection des données ait été le repère mondial pour la gouvernance de l'IA au cours de la dernière décennie, les politiques concernant les systèmes de RF et ainsi de l'IA se réorientent vers le processus décisionnel assisté par l'IA. Dans ce sens, de nombreux nouveaux cadres ont été suggérés, comme des évaluations des risques et de la responsabilité algorithmique pour expliquer certaines des limitations de la gouvernance des données, incluant la distinction trouble entre les renseignements personnels et non personnels. Bien que la protection de la vie privée est une métrique importante pour la confidentialité et la sécurité des données, les, torts potentiels de la RF vont bien au-delà de la protection de la vie privée.[20] Les entreprises doivent assumer non seulement la protection et l'utilisation responsable des données et des renseignements personnels, mais aussi assumer les décisions prises en fonction de l'utilisation de leurs systèmes, surtout quand ces décisions causent des dommages excessifs, de la discrimination, des violations des droits de la personne, et des risques pour les citoyens et citoyennes. Ces risques incluent l'exclusion à l'accès aux ressources et aux soins, et sont d'une importance particulière pour les populations déjà vulnérables et marginalisées.

L'utilisation sécuritaire des systèmes de RF par le secteur public nécessite des critères ciblant plus que le transfert des données à travers les systèmes technologiques, mais aussi des critères qui peuvent rendre compte des acteurs employant ces systèmes et son impact sur la population.[21] Par exemple, le Algorithmic Accountability Act aux États-Unis se focalise sur les prises de décision utilisant l'IA et requiert que « les entreprises évaluent les besoins sécuritaires des données des consommateurs et consommatrices ainsi que l'impact social de leur technologie, et inclue des critères spécifiques pour évaluer la discrimination, les préjugés, l'équité, et la sécurité ».[22] [23] Ceci représente un changement important à la manière dont les lois et politiques axées sur les systèmes algorithmiques approchent la question de l'impact aux droits de la personne.

Considération et questions:

Qui développera et en quoi consistera ce cadre de gouvernance des données?

Ce cadre directeur devrait être plus robuste que les exemples canadiens actuels, comme la LPRPDE, à cause de la nature confidentielle des données de RF et le potentiel de nuisance de la technologie. Le cadre devrait être informé par la politique, le droit, et la technologie, et développé en concert avec des experts et expertes issus de ces domaines. Les responsables politiques doivent déterminer qui prendra responsabilité pour la création d'un tel cadre et qui seront visés par les règlements. Les mécanismes pour répondre aux violations devront également être mis au point.

* Ceux-ci incluent licéité et loyauté, transparence, limitation des finalités, minimisation des données, exactitude, droit d'accès, de rectification, de suppression et d'objection, la limitation de la conservation des données, l'intégrité et la confidentialité, et la responsabilité comme définit au sens large dans l'article 5 du règlement.

LA SÉCURITÉ

Les données de la RF doivent être strictement protégées des acteurs malicieux et des violations technologiques. Les fournisseurs ainsi que les institutions qui se servent de la technologie doivent prendre des mesures de sécurité adéquates, tel le cryptage, l'entreposage central, des réseaux protégés, et des restrictions sur l'accès.

Considérations et questions:

Comment assurer une sécurité adéquate? Quels sont les risques à prévoir?

Les institutions devront être sujet à des contrôles pour évaluer la fiabilité de leurs mesures de sécurité, surtout en tenant compte les histoires émergentes des violations comme celles de Clearview AI.[24] Les risques à la sécurité s'étendent au-delà des attaques de l'extérieur des systèmes: les acteurs au sein des institutions, notamment dans les services de police, doivent également respecter des règlements très stricts pour éliminer la possibilité d'accès non autorisé au service de RF et ses données.

CONDITIONS DE PARTIALITÉ ET D'EXACTITUDE

Des études ont démontré que la RF a une tendance vers la discrimination basée sur l'identité, particulièrement contre les personnes racisées.[25] Les fournisseurs de RF doivent démontrer la précision générale de leurs systèmes de reconnaissance et prouver que leurs taux de faux positifs selon chaque segment démographique (genre, âge, et teint de la peau) concordent avec les critères universels déterminés par le gouvernement.

Considérations et questions:

Quels jeux de données d'essai devraient être utilisés?

Il faudra évaluer la précision et le taux des faux positifs d'un système en employant des jeux de données standardisés et divers. Les auditeurs devront aussi considérer que, si les essais sont effectués en utilisant une petite quantité de jeux de données d'essai disponible au public, les fournisseurs pourront facilement entraîner leurs algorithmes à répondre parfaitement à ces jeux de données. Une alternative consisterait de créer des jeux de données classifiés, sinon la création périodique de nouveaux jeux de données d'essai qui seront seulement rendus accessibles aux entreprises et au public après les contrôles.

Comment seront évalués la précision démographique ainsi que les biais de l'algorithme?

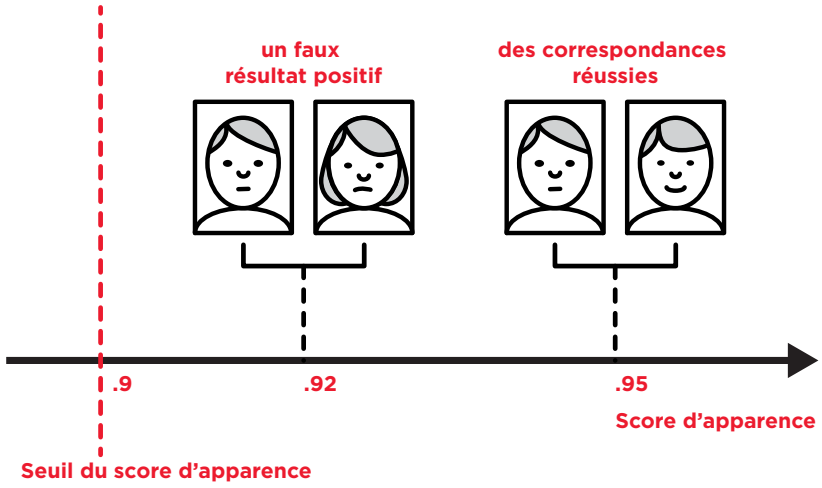
Évaluer la précision et les préjugés des systèmes de RF est une tâche technologiquement difficile. Une méthode précise et systématique pour calculer la précision et les préjugés demeure insaisissable; plus de recherche informatique est nécessaire pour déterminer non seulement la meilleure méthode d'évaluation, mais aussi comment assurer que les algorithmes peuvent réussir.

À la base, la technologie de RF compare des images de visages et trouve chaque correspondance possible entre des paires de photos en générant une note d'apparence pour chaque paire. Le plus haut le score, le plus il est possible que les deux images représentent la même personne. Une identification possible est signalée si la note d'apparence est plus élevé qu'un seuil du score d'apparence donné.

Il y a deux approches principales pour estimer l'exactitude d'un système de RF.

Méthode nº 1

La première méthode évalue chaque paire d'images de visage qui a une note d'apparence plus élevée qu'une note de base particulière, comptant le nombre de ces paires représentant réellement le même visage (des correspondances réussies) et combien ne représentent pas le même visage (des faux positifs). Le taux de faux positifs (le pourcentage des paires signalées comme correspondantes par erreur) est une mesure cruciale; dans le maintien de l'ordre par la police, où les faux positifs peuvent mener à des arrestations arbitraires, un taux extrêmement faible de faux positifs est essentiel.



Les faiblesses de la méthode nº 1

Méthode nº 1 est compliqué par le fait qu'il existe un compromis important entre le taux de faux positifs d'un algorithme de RF et son seuil de score d'apparence. Augmenter le seuil diminue les taux de faux positifs, puisque ça diminue le nombre total de paires dont le score d'apparence dépasse ce seuil (et par extension diminue le nombre de correspondances erronées). Ce seuil peut donc être ajusté pour obtenir le taux de faux positifs désirés.

Pour tester un algorithme, il y a deux options :

1. Tester chaque démographique contre un seuil fixe;
2. Varier le seuil par démographique pour que chaque groupe corresponde à un taux fixe de faux positifs.

Les systèmes actuel de RF vont très probablement mal satisfaire la première option : un papier affilié avec la NIST a récemment trouvé qu'un seuil fixe dans la Méthode nº 2 produit un taux de résultats positifs plus élevé pour les asiatiques de l'Est que les caucasiens ou caucasiennes, reflétant des résultats similaires produit par d'autres études.[26] Par contre, la deuxième approche est également imparfaite : au lieu d'adresser les causes sous-jacentes des préjugés du logiciel, elle déplace les critères pour que chaque démographique semble être traité de manière égale. De plus, cette approche n'est pas convenable pour l'utilisation publique. Par exemple, si utilisé pour chercher à travers une base de donnée d'images (sans renseignement personnel ajouté) capturé par la vidéosurveillance, l'algorithme aura besoin de déterminer quel sera le seuil démographique approprié pour chaque photo individuelle. Ceci nécessiterait ajouter des renseignements démographiques à chaque image, sinon manuellement ou en utilisant un algorithme pour la classification des genres et des races potentiellement biaisée.[27]

Méthode nº 2 et ses lacunes

Une deuxième méthode évite ce compromis difficile en ignorant le seuil du score d'apparence complètement et mesurant à la place la précision « générale » du système, analysant les différences entre chaque score d'apparence calculé par le système. Par contre, cette méthode

a été démontrée comme étant incapable de détecter les préjugés que la première méthode détecte facilement.[28]

Les échecs des deux méthodes

Les deux méthodes sont encombrées par leur dépendance sur des catégorisations démographiques arbitraires. La race, l'âge, et même le genre ne peuvent pas être catégorisés nettement et distinctement. Pour mesurer le préjugé démographique, par contre, une division distincte dans les jeux de données d'essai est nécessaire pour que la précision de chaque groupe distinct (p. ex., masculin ou féminin; jeune, adulte, âgé, etc.) puisse être enregistré. Les photos des individus qui entrent nettement dans une catégorie particulière sont plus susceptibles à être incluses dans les jeux de données pour l'essai, tandis que les personnes de race mixte ou de genre non-binaire sont plus susceptibles à être exclues. Par conséquent, les testeurs risquent de ne pas savoir exactement comment le système de RF va réagir en traitant les données relatives à ces groupes.

De plus, le préjugé peut s'insinuer dans la démarche de catégoriser démographiquement les jeux de données pour l'essai, que la catégorisation soit faite manuellement ou par algorithme.

Comment développer de meilleures méthodes pour évaluer la précision démographique et les tendances biaisées d'un système? Comment peut-on réduire les préjugés des systèmes?

Développer des méthodes convenables pour mesurer la précision et les tendances dans la technologie de RF nécessitera davantage de recherche réalisée par des équipes d'informaticiennes et d'informaticiens travaillant aux côtés des expertes et experts politique et démographique. Mais, pour que le moratoire soit levé, il n'est pas suffisant de posséder les moyens d'évaluer les préjugés : les systèmes de RF doivent être suffisamment neutres pour réussir ladite évaluation. Comme résumé dans l'Exposé no° 1, les causes des préjugés du système (et par extension, comment les résoudre) demeurent peu claires. Davantage de recherche en informatique et dans les sciences humaines est nécessaire pour la réduction des préjugés.

CONDITIONS DE REVUE ET DE SUPERVISION

Préalablement au levé d'un moratoire, un organisme pour la supervision et la révision devrait être établi. Cet organisme devrait être basé sur les Autorités chargées de la protection des données de l'Union européenne des autorités publiques indépendantes chargées avec l'investigation et la correction des violations aux lois protégeant les données.[29] En plus de s'assurer de la supervision de l'application de la loi pour la protection des données, cet organisme canadien pourrait décider comment répondre aux plaintes concernant la vie privée et la protection des données.

LA VÉRIFICATION

La plupart des conditions décrites dans ce document nécessiteront des contrôles réguliers pour assurer qu'elles sont respectées. De nombreuses institutions publiques utilisant la technologie de RF devront être surveillées pour vérifier que les cas d'emploi adhèrent aux règlements, et que la collecte et l'entreposage des données par ou pour des fins de RF sont

adéquatement sécuritaires. Les compagnies qui commercialisent leurs systèmes de RF dans le secteur public doivent aussi soumettre leurs produits à des vérifications pour évaluer leur exactitude et assurer qu'ils respectent les normes établies pour la protection des données et de la vie privée.

Considérations et questions

Qui effectuera cette vérification?

Les responsables politiques doivent déterminer qui va se charger des contrôles des institutions publiques, et si chaque condition (cas d'emploi, utilisation des données, et sécurité) devrait être contrôlée séparément. Les vérificateurs potentiels incluent un organisme public tiers, le Commissariat à la protection de la vie privée du Canada, ou un organisme de réglementation à l'intérieur de chaque institution. Des délibérations semblables devront être menées sur la vérification des fournisseurs privés de la RF. Il faudra aussi déterminer quels seront les pouvoirs détenus par les vérificateurs pour assurer le respect des règlements (p. ex., des amendes ou moratoires sur les contrats gouvernementaux pour les fournisseurs, ou l'imposition des restrictions sur l'utilisation de la RF par les institutions).

Est-ce que les résultats de ces contrôles seront accessibles au public?

Si les résultats de ces évaluations ne sont pas rendus accessibles au public, la confiance du public devra être cultivée d'une autre manière.

CONDITIONS SOCIALES

Les tendances émergentes mondiales démontrent que les populations les plus à risques subissent les conséquences les plus négatives de la RF, comme décrites dans Exposé n° 1. Les impacts sociaux de la technologie de RF devront aussi être analysés, incluant la manière dont la technologie peut affecter toute la société. Les systèmes omniprésents de surveillance publique, par exemple, sont de plus en plus examinés par le public, reflétant les mouvements mondiaux pour la justice raciale et les libertés civiles.[30] Avant de lever un moratoire, le gouvernement canadien devrait mettre au point un outil ou un cadre pour évaluer le bien-fondé social de n'importe quel système de RF. Ceci pourrait inclure une discussion concernant d'autres méthodes moins invasives, mais tout aussi fiables, qui pourront être utilisées pour remplacer les systèmes de RF ou de surveillance biométrique. Un cadre qui serait possiblement approprié sous un moratoire pourrait inclure une analyse des lacunes, comparant la performance actuelle des systèmes existants de RF avec un état futur désiré. Si l'écart entre l'état actuel et le désiré est trop large, un moratoire ne devrait pas être levé.

Considérations et questions

Comment mesurer le bien-fondé social d'un système de RF?

Un cadre pour le bien-fondé social devrait être conceptualisé à partir de recherche et de consultation avec les communautés qui seront les plus touchées par la RF. Il devrait aussi adresser directement les utilisations publiques aux enjeux très importants, notamment l'utilisation de la RF par les forces de l'ordre, et devrait répondre aux questions suivantes :

- ***Comment mesurer l'impact public de la surveillance technologique accrue contre les bienfaits potentiels d'un système de RF?***

- ***Est-ce qu'il existe des exemples d'utilisation actuelle de systèmes de RF en question (ou des systèmes semblables) affectant négativement, causant du tort, ou augmentant l'injustice vécue selon les catégories de la race, de la classe, de la sexualité ou du genre?***

- ***Est-ce que l'objectif de l'utilisation d'un système de RF peut être accompli d'une autre manière?***

CONDITIONS LÉGALES

SPÉCIFIER L'UTILISATION DU SERVICE

La loi sur la protection des renseignements personnels décrit comment les institutions du gouvernement fédéral doivent traiter les données personnelles, dont la collecte, l'utilisation, et le partage peuvent seulement être effectués avec le consentement de l'individu à des fins limitées et légitimes, sauf dans des circonstances très étroites.[31]

Le pouvoir unique des services policiers est sujet à des mécanismes supplémentaires de protection. Par exemple, la collecte d'informations biométriques au moment d'une arrestation, telles les empreintes digitales, est gouvernée par la Loi sur l'identification des criminels[32] et la collecte des substances corporelles pour l'analyse ADN est réglementée par le Code criminel[33] et nécessite un mandat (des lois supplémentaires comme celles trouvées dans la Loi sur le Service canadien du renseignement de sécurité et la Loi sur les douanes peuvent aussi prendre effet, en fonction du contexte).

Ces provisions ne s'appliquent pas à l'utilisation policière des images biométriques numériques à travers les RF, signifiant que ces images peuvent être récupérées sans le consentement de l'individu et la supervision de la cour.

MODIFICATION AU CODE CRIMINEL

Le Gouvernement du Canada devrait contempler la modification du Code criminel pour mettre l'utilisation de la technologie de RF sous les mêmes protections régissant les caractéristiques biométriques comme les empreintes digitales et les substances corporelles utilisées pour l'analyse ADN. Ceci rendrait les preuves récupérées par la technologie de RF inadmissible à la cour, à moins qu'une démarche standardisée et particulière ait été suivie pour la collecte et l'entreposage des renseignements (en particulier, le besoin d'un mandat).

MODIFICATION À LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les droits détenus par les Canadiens et Canadiennes prévus par la loi ne devraient pas être différents pour les données récupérées par la technologie de RF. Le caractère dissimulé de l'observation par la technologie de RF empêche l'individu de maintenir le contrôle sur la manière dont il est surveillé, ainsi que sur la façon dont ses renseignements personnels sont utilisés.[34] Clarifier l'ambiguïté entourant l'applicabilité des provisions légales actuelles à la technologie de RF est une priorité.

PROCHAINES ÉTAPES : RECHERCHE ET ÉTUDES PENDANT UN MORATOIRE

Les sections précédentes ont souligné les conditions technologiques, sociales, politiques, et juridiques qui doivent exister avant le levé d'un moratoire sur la technologie de RF. Elles ont aussi décrit les considérations et questions soulevées par ces conditions, qui nécessitent toutes beaucoup de recherche ou de délibération. Cette section énumère les étapes que le gouvernement canadien devrait entreprendre lors d'un moratoire pour étoffer ces conditions et adresser leurs considérations et questions. Lever un moratoire sans avoir suivi ces étapes (ou des étapes substantivement semblables) serait peu judicieux, puisque de nombreuses conditions importantes (notamment assurer un faible degré de préjugé) ne seront pas remplies, tandis que d'autres conditions (telle la création d'un cadre de gouvernance des données) sont difficiles à définir et développer sans davantage de consultation et de recherche.

PANEL MULTISECTORIEL

Le gouvernement du Canada devrait rassembler un panneau d'experts et d'expertes de haut niveau composé de spécialistes politiques, technologiques, sociologiques, et juridiques. Ce panneau aura la responsabilité de développer les conditions régulatrices optimales pour lever un moratoire, construites à partir des conditions, questions, et considérations énumérées dans ces exposés. Leur mandat devrait également inclure l'étude de l'utilisation actuelle de la technologie de RF au Canada et une revue des données et des lois actuelles sur la protection et la vie privée pour identifier les lacunes.[35] Ce panneau mené par des experts et expertes pourrait conduire les consultations, la recherche, et les projets d'évaluation, comme décrits ci-dessous.

CONSULTATIONS À TRAVERS LE CANADA

Le gouvernement fédéral devrait mener des consultations à grande échelle pour évaluer les perspectives des Canadiens et Canadiennes—particulièrement ceux et celles appartenant aux communautés marginalisées—sur l'utilisation publique de technologie de RF, notamment par les services de police. Les acteurs clés engagés par ces consultations devront inclure: les groupes de revendication, les associations de liberté civile nationales et internationales, les commissaires fédéraux et provinciaux pour la défense de la vie privée, les représentants et représentantes des comités et organismes fédéraux appropriés, ainsi que les services de police municipales, provinciales, et fédérales.[36] Cette approche, qui est en ligne avec les démarches politiques du gouvernement fédéral sur la technologie et la vie privée, donnerait aux responsables politiques la capacité à privilégier la protection des droits de la personne.[37]

La coordination de la consultation par le gouvernement fédéral assurera l'uniformité de l'information fournie aux différents niveaux du gouvernement. Le résultat principal de ces consultations devrait être une évaluation de la désirabilité de l'utilisation de la technologie de RF par les forces de l'ordre, plutôt que des propositions pour modifier les lois existantes protégeant la vie privée et les renseignements personnels.

COMITÉ DE LA RECHERCHE INTERDISCIPLINAIRE

À la suite des consultations, le gouvernement fédéral devrait maximiser les perspectives rassemblées pour coordonner un effort de recherche nationale sur l'utilisation de la technologie de RF par le secteur public, se concentrant sur l'impact de la RF sur les communautés racisées. Cet effort de recherche servira à renforcer la transparence quant à l'utilisation policière actuelle de la technologie de RF, adressant le manque sérieux de données qui fait actuellement obstacle à l'élaboration de politiques et de règlements sur la RF.

Une série de rapports, chacune cadrant ses investigations à travers une approche axée sur les droits de la personne, pourrait être commissionnée par le Commissariat à la protection de la vie privée du Canada, les commissaires provinciaux, et le Conseil national de recherches Canada. Le plus important de cette série serait un rapport compréhensif détaillant quels organismes canadiens, aux niveaux fédéraux, provinciaux/territoriaux, ou municipaux, ont utilisé ou testé des systèmes de RF et à quelles fins, incluant une analyse des risques et bienfaits possibles pour la société. Ce rapport compréhensif devrait indiquer les résultats et les leçons apprises au cours de l'investigation sur la GRC et la technologie de RF effectuée par le Commissariat à la protection de la vie privée. Un deuxième rapport devrait examiner chaque système de RF vendu au Canada pour déterminer si une sensibilisation accrue des risques et préjugés de la RF a suscité des améliorations de la technologie.

Obtenir accès aux données détaillées et désagrégées sur les lacunes de la technologie de RF actuelle est primordial pour obtenir l'engagement des acteurs clés, notamment les services de police fédéraux et municipaux sur le besoin de la réglementation. Effectivement, sans information suffisante sur l'utilisation actuelle de la technologie de RF, il est difficile de convaincre les forces de l'ordre de la nécessité d'une réforme. Cette série de rapports pourrait également situer le Canada comme leader mondial dans l'effort de combler la brèche de connaissances entourant les incidences éthiques et les conséquences pour les droits de la personne suscitées par l'utilisation policière de la RF.

Le financement fédéral devrait également être donné aux universités et aux instituts de recherche pour conduire des études, notamment sur le sujet des biais algorithmiques et ses causes sous-jacentes, ainsi que les solutions proposées. Pour recevoir ce financement, des conditions explicites pour le partage des perspectives, code, et techniques avec un comité consultatif doivent être établies. Comme décrit dans le Plan ministériel de Sécurité publique Canada 2019-2020, des nouvelles conditions incluant mais non limité à « tenir des discussions avec les provinces et territoires pour identifier les établissements qui ont besoin d'être réhabilités immédiatement »38 ont été développé à la réception du financement. Le gouvernement fédéral devrait aussi fournir son appui financier aux efforts des provinces à évaluer l'utilisation policière de la RF.

ÉVALUATION DES CONSÉQUENCES SUR LA VIE PRIVÉE ET LA PROTECTION DES DONNÉES

Les évaluations des facteurs à la vie privée (EFVP) par le Commissariat à la protection de la vie privée au Canada évaluent les utilisations actuelles de la technologie de RF pour assurer qu'elles conforment aux lois fédérales sur la vie privée comme décrites dans la Loi sur la protection des renseignement personnels. Depuis 2004, le Commissariat à la protection de la vie privée a mené des EFVP sur le Projet

de reconnaissance faciale de Passeport Canada, avec des recommandations pour atténuer les atteintes à la vie privée des programmes fédéraux[38] Avant de lever le moratoire, des EFVP sur chaque organisme gouvernemental axées sur une analyse du besoin justifiable et l'utilisation cohérente (voir les Conditions des intentions), l'accès, le stockage, et la sécurité (voir les Conditions sur l'utilisation des données), et l'exactitude et le biais algorithmique devraient être réalisées. Semblable aux EFVP, les, Analyse d'impact relative à la protection des données (AIPD) évaluent les risques liées aux données et vérifient que les lois sur la protection des données sont respectées;40 des AIPD devraient également être effectuées.

CONCLUSION

La réussite d'un moratoire repose sur la confiance publique. La transparence gouvernementale doit être privilégiée à chaque étape de la démarche décisionnelle : en établissant le moratoire, en l'évaluant des systèmes de RF, et à travers la mise en œuvre des conditions avant de lever le moratoire. Toute recherche, consultation, et évaluation effectuée pendant le moratoire devraient être rendues publiques, et leurs résultats partagés avec les citoyens et citoyennes de manière accessible. Le gouvernement du Canada devrait également appuyer les efforts pour améliorer les connaissances informatiques, équipant les Canadiens et Canadiennes avec le savoir sur leurs propres droits et responsabilités numériques. Nous encourageons le Canada à servir comme modèle de leadership mondial pour le développement et la mise en œuvre des conditions technologiques, sociales, politiques et juridiques spécifiques qui doivent être remplies avant que tout moratoire futur sur la technologie de RF puisse être levé.

RÉFÉRENCES

1 The Canadian Press. "NDP Calls for Moratorium on Clearview AI Facial Recognition Software." National Post, March 9, 2020, https://nationalpost.com/pmn/news-pmn/canada-news-pmn/ndp-calls-for-moratorium-on-clearview-ai-facial-recognition-software.

2 Taylor Owen and Nasma Ahmed. "Opinion: Let's Face the Facts: To Ensure Our Digital Rights, We Must Hit Pause on Facial-Recognition Technology." The Globe and Mail, February 14, 2020, https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/.

3 Jay Greene. "Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM." The Washington Post, June 11, 2020, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

4 Mark Montgomery. "National Police to limit, but not stop use of facial recognition technology." RadioCanada International. March 10, 2020, https://www.rcinet.ca/en/2020/03/10/national-police-to-limit-but-not-stop-use-of-facial-recognition-technology/.

5 Office of the Privacy Commissioner of Canada. "Clearview AI ceases offering its facial recognition technology in Canada." July 6, 2020, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/.

6 Kashmir Hill. "Wrongfully Accused by an Algorithm." The New York Times, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

7 Bobby Allyn. "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man." NPR, June 24, 2020, https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

8 National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, by Patrick Grother, Mei Ngan, and Kayee Hanaoka, Rep. 8280, US Department of Commerce, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (accessed July 8, 2020).

9 Office of the Privacy Commissioner of Canada. "PIPEDA Fair information principles." May 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.

10 Amba Kak and Rashia Richardson. "The Office of the Privacy Commissioner of Canada Consultation: Proposals for ensuring appropriate regulation of artificial intelligence." p. 11. AINow. March 12, 2020, https://ainowinstitute.org/ainow-comments-to-canadian-office-of-the-privacy-commissioner.pdf.

11 Ibid

12 Office of the Privacy Commissioner of Canada. "Consent." September 10, 2019, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/.

13 Heide Pearson. "Calgary mall defends use of facial-recognition technology after customer discovers they're being watched" Global News, July 28, 2018, https://globalnews.ca/news/4355444/chinook-mall-calgary-facial-recognition-technology/.

14 Kate O'Flaherty. "Clearview AI's Database Has Amassed 3 Billion Photos. This Is How If You Want Yours Deleted, You Have To Opt Out." Forbes, January 26, 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/01/26/clearview-ais-database-has-amassed-3-billion-photos-this-is-how-if-you-want-yours-deleted-you-have-to-opt-out/#5665f59660aa.

15 Ben Wolford. "Everything you need to know about the 'Right to be forgotten'" GDPR.eu, accessed July 16, 2020, https://gdpr.eu/right-to-be-forgotten/.

16 Thomas Daigle. "Canadians can now opt out of Clearview AI facial recognition, with a catch." CBC News, July 10, 2020. https://www.cbc.ca/news/technology/clearview-ai-canadians-can-opt-out-1.5645089.

17 SAS. "The SAS Data Governance Framework: A Blueprint for Success." p. 5 2018. https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/sas-data-governance-framework-107325.pdf.

18 World Economic Forum. "A Framework for Responsible Limits on Facial Recognition" February 2020. http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf.

19 Theodore Christakis. "First Ever Decision of a French Court Applying GDPR to Facial Recognition." AI-Regulation, February 27, 2020, https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/#:~:text=First%20Ever%20Decision%20of%20a%20French%20Court%20Applying%20GDPR%20to%20Facial%20Recognition&text=A%20French%20court%20canceled%20today,that%20this%20would%20be%20illegal.

20 AI Now. "The Office of the Privacy Commissioner of Canada Consultation: Proposals for ensuring appropriate regulation of artificial intelligence" March 2020, https://ainowinstitute.org/ainow-comments-to-canadian-office-of-the-privacy-commissioner.pdf.

21 Ibid.

22 Ibid.

23 US Congress, House, Algorithmic Accountability Act of 2019, HR 2231, 116th Cong., introduced in House April 10, 2019, https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info.

24 Alfred Ng. "Clearview AI's entire client list stolen in data breach." CNET, February 26, 2020, https://www.cnet.com/news/clearview-ai-had-entire-client-list-stolen-in-data-breach/.

25 National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, by Patrick Grother, Mei Ngan, and Kayee Hanaoka, Rep. 8280, US Department of Commerce, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (accessed July 8, 2020).

26 Jacqueline Cavazos, P. Jonathon Phillips, Carlos D. Castillo, and Alice J. O'Toole. "Accuracy comparison across face recognition algorithms: Where are we on measuring race bias?" NSIST, June 4, 2020, https://arxiv.org/pdf/1912.07398.pdf.

27 Joy Buolamwini and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," (paper presented at 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research), 81:77-91, 2018. https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf.

28 Ibid.

29 European Commission. "What are Data Protection Authorities (DPAs)?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en.

30 Tawana Petty. "Defending Black Lives Means Banning Facial Recognition." Wired, July 10, 2020, https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/.

31 Privacy Act, Revised Statutes of Canada 1985, c. P-21. https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-p-21/161168/rsc-1985-c-p-21.html#sec2.

32 Identification of Criminals Act, Revised Statutes of Canada 1985, c. I-1. https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-i-1/161284/rsc-1985-c-i-1.html#sec2.

33 Criminal Code, Revised Statutes of Canada 1985, c. 46. https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-46/161288/rsc-1985-c-c-46.html#sec487.05.

34 Office of the Information & Privacy Commissioner for British Columbia, Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia. Elizabeth Denham. February 16, 2012. https://www.oipc.bc.ca/investigation-reports/1245.

35 Taylor Owen and Nasma Ahmed. "Let's face the facts: To ensure our digital rights, we must hit pause on facial-recognition technology." The Globe and Mail, February 14, 2020, https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/.

36 Nani Jansen Reventlow. "How Amazon's Moratorium on Facial Recognition Tech Is Different From IBM's and Microsoft's". Slate, June 11, 2020, https://slate.com/technology/2020/06/ibm-microsoft-amazon-facial-recognition-technology.html.

37 "Canada's Digital Charter: Trust in a digital world," Government of Canada, June 8, 2020, https://www.ic.gc.ca/eic/.site/062.nsf/eng/h_00108.html.

38 Office of the Privacy Commissioner of Canada, Automated Facial Recognition in the Public and Private Sectors, Gatineau, QC, 2014, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf.