TECH INFORMED POLICY

LE 18 AOÛT 2020

EXPOSÉ Nº 1 SUR UN MORATOIRE SUR LA RECONNAISSANCE FACIALE

Implications d'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.

Identification faciale : Un système de reconnaissance faciale qui compare une photo à plusieurs photos de différentes personnes. Cherche à répondre à la question : « Qui est cette personne ? »

Information accessible au public : Information facilement accessible à travers l'internet, les réseaux sociaux, etc.

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.

Vérification faciale : Un système de reconnaissance faciale qui compare une photo à plusieurs photos de la même personne. Cherche à répondre à la question : « Est-ce la même personne ? »

SOMMAIRE EXÉCUTIF :

Ce document est le premier de deux exposés sur la technologie de reconnaissance faciale (RF). Celui-ci aborde comment la RF fonctionne et est utilisée, ainsi que les implications d'un moratoire fédéral, tandis que le deuxième, exposé nº 2, explore les conditions nécessaires pour lever ledit moratoire.

- Depuis le mois de mars 2020, des appels montent pour que le Canada impose un moratoire national sur la technologie de reconnaissance faciale, surtout en ce qui concerne les entreprises fournissant les systèmes de RF aux forces de l'ordre.[1] [2] [3]
- Un moratoire national permettrait aux responsables législatifs plus de temps pour mettre au point une politique efficace et compréhensive réglementant la conception, l'utilisation, et la distribution des systèmes de RF ainsi que la manière dont les données sont collectées, utilisées, et partagées.
- Les systèmes de RF actuels ne sont pas infaillibles. Les services de police ne peuvent pas dépendre sur ces systèmes à cause de leur potentiel discriminatoire et inéquitable contre certaines démographies.
- Ce document résume les conditions technologiques, sociales, politiques, et juridiques nécessaires pour lever un moratoire canadien sur les systèmes de RF. La discussion souligne les préoccupations, limites, et préjudices potentiels de la RF, ainsi que les implications techniques d'un moratoire fédéral. Le deuxième document conclura avec une analyse des conditions techniques, sociales, et politiques requises pour lever un moratoire fédéral ainsi que des recommandations pour utiliser les systèmes de RF de manière sécuritaire.

QU'EST-CE QUE LA TECHNOLOGIE DE RECONNAISSANCE FACIALE (RF) ?

La reconnaissance faciale décrit le processus nécessaire pour identifier un visage à partir d'une image ou d'un enregistrement vidéo en format numérique. La technologie de RF utilise l'intelligence artificielle (IA) pour identifier les caractéristiques particulières du visage d'une personne et tente ensuite de retrouver ces mêmes caractéristiques dans d'autres images.

COMMENT EST-CE QUE LA RF FONCTIONNE ?

Les systèmes de RF peuvent être divisés en deux catégories : les algorithmes de vérification et d'identification.

Un algorithme de vérification compare l'image d'une personne contre multiples images d'une même personne pour vérifier l'identité de la première. Déverrouiller un téléphone avec la RF est une utilisation typique de la vérification.

Un algorithme d'identification compare l'image d'une personne contre une base de données de visages différents et cherche ainsi à identifier un individu à partir de son visage. Les services policiers et frontaliers emploient ce type d'algorithme, donc ce document se concentra sur cet aspect de la RF.

Un système d'identification faciale comprend les parties suivantes :

- Une base de données d'images photographiques de visages. Cette base de données peut appartenir à une agence gouvernementale (p. ex., la collection de clichés anthropométriques utilisée la police), ou peut être fournie par les créateurs du système (p. ex., une banque d'images trouvées sur l'internet par la compagnie de RF).
- Un algorithme, qui traite la photographie d'un visage et tente de trouver des visages correspondants parmi les images d'une base de données.
- Un jeu de données d'entraînement d'images de visages utilisé par les développeurs et développeuses pour entraîner le système à effectuer des identifications exactes.
- Un jeu de données d'essai pour tester l'exactitude de l'algorithme.

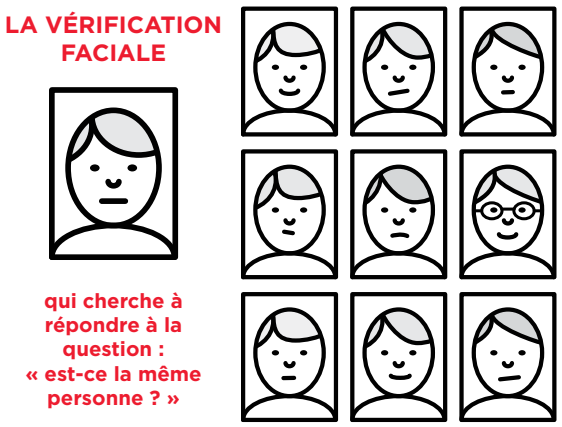
Étape 1 – extraction des caractéristiques : Un algorithme basé sur l'intelligence artificielle calcule une représentation numérique d'un visage en extrayant la forme, la taille et la distance relative entre ses caractéristiques. Cette représentation numérique s'appelle un vecteur de caractéristiques. Précisément comment et quelles caractéristiques sont chiffrées peut être assez insondable, puisque les développeurs et développeuses ne définissent pas concrètement les caractéristiques ciblées, c'est l'algorithme qui « apprend » à les définir. Avant son déploiement, l'algorithme est entraîné et testé avec de très grandes collections d'images. Après son déploiement, selon les conditions de service du système de RF, les images ainsi que d'autres métadonnées utilisées peuvent être récupérées par les fournisseurs pour entraîner d'autres systèmes.[4]

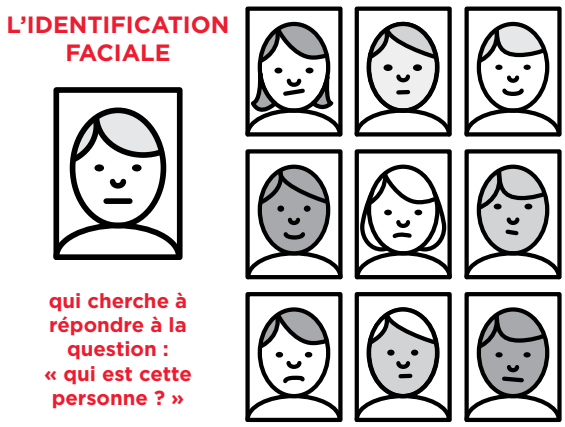
Étape 2 – comparaison des caractéristiques : Après le calcul du vecteur de caractéristiques, le système de RF le compare aux vecteurs calculés pour chaque image dans une base de données. Chaque paire de vecteurs comparés est donnée un score d'apparence : plus ce dernier est élevé, plus il est probable que les deux images représentent la même personne.

Une comparaison de deux images est signalée comme potentiellement correspondante si le score d'apparence de la paire est plus élevé que le seuil du score d'apparence. Certaines tâches, comme l'identification d'un criminel, nécessitent un très haut degré de certitude et ont une très faible tolérance d'erreur. Ces tâches nécessitent un seuil élevé, pour que seulement les paires très possiblement identiques soient signalées. Pour d'autres tâches, comme l'identification automatique des utilisateurs et utilisatrices Facebook dans leurs photos, un seuil moins élevé est acceptable. Puisqu'un système commercial de RF est souvent utilisé pour accomplir différentes tâches avec des besoins de confidentialité différents, aucun seuil du score d'apparence standard à travers l'industrie ne peut être établi.[5] Un seuil par défaut est fixé les développeurs et développeuses mais peut être ajusté par l'institution.*

* L'ACLU a trouvé que Rekognition, système de RF conçu par Amazon, a identifié 28 membres du congrès parmi les photographies anthropométriques utilisées par la police lorsque le seuil du score d'apparence était réglé à 80%; Amazon a répondu que le réglage recommandé pour les services de police est 95%. Par contre, il n'existe aujourd'hui aucun mécanisme pour faire respecter cette recommandation parmi les services de police qui utilisent les systèmes de RF.*

* L'ACLU a trouvé que Rekognition, système de RF conçu par Amazon, a identifié 28 membres du congrès parmi les photographies anthropométriques utilisées par la police lorsque le seuil du score d'apparence était réglé à 80%; Amazon a répondu que le réglage recommandé pour les services de police est 95%. Par contre, il n'existe aujourd'hui aucun mécanisme pour faire respecter cette recommandation parmi les services de police qui utilisent les systèmes de RF.





UTILISATION RÉCENTE DE LA TECHNOLOGIE DE RF AU CANADA

UTILISATION RÉCENTE PAR LE GOUVERNEMENT

Protection frontalière du Canada :

Aux aéroports majeurs comme l'Aéroport international de Vancouver ou l'Aéroport international Pearson de Toronto, l'Agence des services frontaliers du Canada (ASFC) fournit des kiosques libre-service volontaires aux douanes pour vérifier l'identité des voyageurs et voyageuses entrant au pays. Les membres des programmes NEXUS[6] ou CANPASS peuvent aussi être vérifiés à travers une identification volontaire de l'iris.[7] Cette technologie, nommée

BorderXpress, est fournie par Innovative Travel Solutions, une entreprise affiliée à l'Aéroport international de Vancouver.[8] Elle envoie les informations pertinentes à l'ASFC, mais ne garde pour elle-même aucune information personnelle. Passeport Canada utilise aussi la RF pour évaluer la légitimité des demandes de passeport.[9]

Municipal police departments:

Un minimum de 35 départements de police ont fait recours à la technologie de RF.[10] Le Service de police de Calgary (CPD) utilise NeoFace Reveal depuis 2014 pour comparer les images et vidéos des suspects potentiels, notamment tirés des enregistrements de vidéosurveillance, contre leur propre base de données de photos d'identité.[11] La CPD respecte des règles strictes concernant la manière dont la RF est utilisée, surtout relatif aux membres du personnel qui ont la permission de l'accéder, ainsi pour s'assurer les images soient seulement comparées aux photos de suspects.[12] Depuis mai 2019 le Service de police de Toronto (TPD) utilisait la technologie de RF de manière similaire au CPD, mais a depuis cessé son utilisation et a soumis une requête d'investigation de Clearview AI, fournisseur de la technologie, au Commissariat à la protection de la vie privée au Canada.[13]

La GRC :

Le Centre national contre l'exploitation d'enfants, division de la GRC, utilisait la technologie RF fournie par Clearview AI afin « d'identifier, de localiser, et de sauver les enfants qui sont ou ont été victimes d'abus sexuel en ligne ».[14] Depuis le 4 mai 2020, le Centre a utilisé le système dans 15 cas et ont sauvé 2 enfants.[15] De plus, certaines équipes au sein de la GRC ont utilisé la technologie à titre d'essai pour tester son « efficacité potentielle au cours des investigations criminelles ».[16] La GRC a déclaré qu'elle aurait utilisé la technologie de RF seulement « dans des circonstances très limitées et spécifiques ».[17]

La technologie de RF est aussi utilisée dans certaines provinces pour comparer des images à celles dans les bases de données des permis de conduite pour empêcher l'usurpation d'identité et la fraude.[18] Certains casinos à travers le Canada utilisent également des caméras de sécurité équipées de technologie de RF pour identifier des tricheurs ou tricheuses connus, ainsi que les personnes qui ont avisé aux casinos qu'elles essaient d'arrêter de jouer.[19]

LE SECTEUR PRIVÉ

La technologie de RF est utilisée également par le secteur privé. Les téléphones intelligents Android et Apple peuvent être déverrouillés par le visage de l'utilisateur ou l'utilisatrice, tandis que Facebook, Google, et Apple utilisent la technologie de RF pour identifier les individus dans les photos téléversées sur leurs plateformes. De plus, certains centres de magasinage, comme le Centre Eaton à Toronto et Canadian Tire, utilisent la technologie de RF pour diminuer les vols à l'étalage.[20] [21] Bell a aussi dévoilé un plan pour la création d'un service de RF destiné aux entreprises canadiennes.[22]

LES ENTREPRISES MAJEURES IMPLIQUÉES DANS LA TECHNOLOGIE DE RF

Amazon :

Amazon fournit son propre système de RF, Rekognition.[23] Rekognition peut identifier des objets, des visages, des textes, des activités, ou du contenu inapproprié représenté dans des images ou vidéos. Le service peut être adapté à plusieurs types d'utilisation et de fonctions au besoin du client. Amazon fournissait Rekognition aux services de police américains, mais a récemment imposé un moratoire d'un an en vue du mouvement Black Lives Matter.[24] [25]

Axon :

Malgré le fait qu'Axon a déjà fourni de la technologie IA aux services de police, la compagnie a trouvé que la technologie de RF n'est ni fiable ni impartiale, et manque de réglementation pour que les forces de l'ordre puissent s'en servir de manière éthique.[26]

Clearview AI :

Le plus grand fournisseur de la technologie de RF aux services de police au Canada était Clearview AI, une compagnie de logiciel américaine.[27] La compagnie a depuis suspendu ses services au Canada, incluant avec la GRC, en réponse à l'investigation en cours réalisée par le Commissariat à la protection de la vie privée.[28]

Clearview AI fourni des services et essais gratuits aux services de police. Le logiciel compare les images téléversées au système contre leur propre base de données, compilée à parti de 3 milliards d'images de visage accessible sur l'internet (tirées de Facebook, Instagram, et autres sites web tiers) sans le consentement explicite des usagers et usagères. Le logiciel retourne alors les autres images du sujet ainsi que l'endroit où ces images ont été trouvées.

L'approche à la vie privée de Clearview AI est discutable. Son utilisation des images aux réseaux sociaux pour les fins de la technologie de RF enfreint les conditions d'utilisation de nombreux sites web, incluant Facebook et Twitter.[29] Clearview AI ne respecte pas les normes de transparence, puisque que la compagnie ne publie aucun détail sur le fonctionnement de leur technologie ni sur son efficacité quant à l'identification exacte des individus. Clearview AI fournissait auparavant leurs services au secteur privé, mais a depuis déclaré que la compagnie travaillera seulement avec les forces de l'ordre dans le futur.[30]

Bien que Clearview AI ait accepté à permettre aux usagers et usagères de demander que leurs photos soient retirées des bases de données après un tollé, ce droit est seulement donné aux personnes résidant dans les juridictions avec des lois existantes gouvernant la technologie de RF, comme la Californie, le Royaume-Unis, et l'Union européenne. Clearview AI a récemment donné aux Canadiens et Canadiennes cette possibilité, malgré le fait que le Canada n'a aucune législation requise.[31]

Facebook :

Facebook a créé DeepFace, leur propre algorithme de RF, en 2014.[32] L'algorithme fut entraîné en le testant avec 4 millions d'images téléversées à Facebook par plus de 4 000 utilisateurs et utilisatrices du site. DeepFace trace les caractéristiques du visage d'une personne à partir d'une image bidimensionnelle et utilise les vecteurs calculés pour créer une représentation

en trois dimensions de la personne. Le logiciel utilise alors cette représentation en trois dimensions pour identifier les autres photos d'une personne sous des angles différents. Apparemment, DeepFace a un taux d'exactitude de 97,25%[33]

Facebook utilise sa technologie de RF pour assister les utilisateurs et utilisatrices du site à identifier les photos de leurs connaissances, à prévenir l'utilisateur ou l'utilisatrice s'il ou elle a été identifié dans une photo téléversée au site, et à protéger contre le mésusage des photos.[34] La Federal Trade Commission américaine a poursuivi Facebook pour une somme de 5 milliards de dollars américains en 2012, notamment pour avoir mal informé leurs usagers et usagères sur l'utilisation de la RF par le site, entre autres violations à la vie privée.[35]

Pour l'instant, Facebook ne commercialise pas DeepFace.

Google :

Google utilise une panoplie de services pour détecter les visages. Les nouveaux téléphones Google peuvent être déverrouillés par le visage de leur utilisatrice ou utilisateur;[36] Google Photos regroupe les visages pour organiser les photos figurant des visages similaires;[37] l'API Google Cloud Vision peut détecter les caractéristiques faciales clés d'une personne à partir de leur image, ainsi que leurs émotions;[38] Google Maps peut détecter les visages qui apparaissent dans « Street View » afin de les anonymiser.[39]

D'après certaines informations, la technologie de RF par Google est plus erronée lorsqu'elle doit détecter des teints plus foncés. Par conséquent, Google a prétendument ciblé des personnes racisées pour qu'elles acceptent de fournir leur image pour améliorer la base de données de la compagnie.[40] Google ne commercialise pas sa technologie de RF au public, mais la compagnie fournit certains autres services à base d'algorithmes d'intelligence artificielle aux services de police à des fins de surveillance.[41]

Idemia :

Idemia a récemment offert leurs services de RF à la Sûreté du Québec. Comme une des plus grandes compagnies d'authentification biométrique au monde, elle fournit sa technologie de RF et de sécurité biométrique aux forces de l'ordre, aux services de sécurité, aux institutions financières, et aux agences gouvernementales à travers le monde.[42] Idemia offre toutes sortes de services d'authentification et de sécurité biométrique, notamment la vidéosurveillance équipée de RF, la reconnaissance et authentification faciale, la vérification de l'identité, des outils de RF en temps réel, et la vérification avancée d'empreintes digitales.[43]

Idemia est basé en France et est donc sujet au Règlement général sur la protection des données (RGPD).[44] Son algorithme a aussi été prouvé dix fois plus erroné quant à l'authentification des personnes racisées que des personnes blanches.[45]

Microsoft :

Microsoft est également un fournisseur important de la technologie de RF au Canada, mais principalement pour le secteur privé. La compagnie offre des essais gratuits de son API Azure pour encourager les équipes de développement de logiciels à intégrer la technologie de RF dans leurs applications. Microsoft ne fournit aucune base de données de recherche, et encourage plutôt les développeuses et développeurs du API Azure à comparer les images contre leurs propres base de données

figurant un maximum de 1 millions d'individus. L'API Azure peut aussi reconnaître des visages similaires et des caractéristiques récurrents parmi les images, ainsi qu'identifier des émotions comme la joie, la colère, et la peur.[46]

Azure détient le plus grand nombre de certificats vérifiant sa conformité aux normes de sécurité que toute autre plateforme cloud d'authentification faciale. Microsoft a aussi déclaré un moratoire sur la prestation de ses systèmes de RF aux services de police.[47]

NEC :

NeoFace Reveal par NEC est actuellement utilisé par le Service de police de Calgary et a été essayé par le Service de police d'Ottawa.[48] NeoFace est considéré par l'Institut national américain des normes et de la technologie (NIST) comme étant la technologie de RF la plus « exacte » actuellement sur le marché.[49] Le système peut améliorer les images de mauvaise qualité et comparer les visages, même à partir d'angle non idéal ou à faible éclairage, aux visages trouvés dans les bases de données des services de la police.[50] Les solutions de sécurité biométriques de NEC sont utilisées par les services de sécurité et les forces de l'ordre dans plus de 70 pays.[51]

Autres entreprises qui fournissent des services de RF :

- Accenture
- Aware
- BioID
- Certibio
- Fujitsu
- Fulcrum Biometrics
- Thales
- HYPR
- Lydos
- M2SYS
- NEC
- Nuance
- Phonexia
- Smilepass

LES ENJEUX AUTOUR DE LA TECHNOLOGIE RF

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

Bien que certains fournisseurs des systèmes de RF n'offrent pas accès à leur base de données de recherche, d'autres oui. Certaines entreprises, notamment Clearview AI, remplissent leurs bases de données en raclant le web pour y recueillir des photos, extrayant des quantités énormes d'information à partir des réseaux sociaux.[52] Ces deux approches diffèrent considérablement: la première permet aux services de police à plus facilement parcourir leurs propres bases de données; la deuxième permet aux comparaisons d'être effectuées avec toute personne ayant une présence visuelle sur le web. Le raclage du web soulève des questions importantes pour la vie privée; LinkedIn et Twitter comptent parmi les géants du web qui agissent contre la pratique, ayant envoyé des mises en demeure à Clearview AI.[53] [54] De nombreuses poursuites ont été lancées contre ce dernier.[55] Malgré son retrait du marché canadien, sa présence autrefois omniprésente au sein des départements de police a souligné les limites des lois actuelles pour la protection des données au Canada, notamment l'échec de fournir aux canadiens et canadiennes le « droit à l'oubli ». Il est possible que le manque de protection adéquate des données soit la raison que Clearview AI ait pu établir une présence aussi forte avec les services de police canadiens. Pour protéger complètement les droits à la vie privée et l'identité des Canadiennes et Canadiens, des règlements révisés et plus fermes sur la protection des données sont nécessaires, ainsi que des règlements capables à mitiger le tort causé par le raclage du web et autres pratiques similaires.

LE CRYPTAGE ET LA SÉCURITÉ DES DONNÉES

En raison de la croissance des atteintes à la protection des données, les entreprises qui fournissent des systèmes de RF aux services de police doivent mettre en place des mesures pour la protection des données et améliorer la sécurité de leurs bases de données.[56]

En février 2020, des stations de police à travers Toronto, employant la technologie de RF par Clearview AI, ont signalé une atteinte de sécurité compromettant « des listes de clients, le nombre de comptes d'utilisateur créé par ces derniers ainsi que le nombre de recherches effectuées ».[57]

Un incident similaire s'est produit aux Royaume-Unis en 2019. Après une vérification par essais de pénétration réalisée par des consultants de sécurité, les stations de police utilisant le système de RF par Suprema ont déterminé que les données étaient sans protection et que les renseignements personnels, incluant notamment « les empreintes digitales de plus d'un million de personnes, ainsi que l'information de reconnaissance faciale, des comptes d'utilisateurs et mots de passe non chiffrés, et l'information personnelle des employés et employées »,[58] étaient facilement accessibles. Les consultants ont pu accéder « l'information dans la base de données du système en manipulant les critères de recherche de l'URL in dans Elasticsearch ».[59] Ces deux exemples démontrent l'importance cruciale des pratiques de cryptage et de sécurité des données pour assurer que les renseignements personnels collectés par la technologie de la RF sont protégés en toute sécurité.

LE PENCHANT STRUCTUREL À L'ÉGARD DES RÉSULTATS PRÉJUDICIELS CAUSANT DU TORT HORS LIGNE

La technologie de reconnaissance faciale—et l'IA en général—a longtemps été susceptible à la partialité et les préjugés basés sur l'identité. Une étude majeure des trois principaux algorithmes de classification de genre a trouvé que malgré leur taux de précision général presque parfait, l'algorithme se trompait jusqu'à 35% du temps sur le genre des femmes aux complexions plus foncées.[60]

Un rapport compréhensif par l'Institut national américain des normes et de la technologie (NIST) axé en particulier sur la technologie de reconnaissance faciale a testé 189 algorithmes sur 18 millions de photos, divisés entre quatre jeux de données.[61] Le rapport a révélé des taux notamment plus élevés de faux positifs (c'est-à-dire, des correspondances erronées) parmi les images de visas des personnes venant de l'ouest et de l'est de l'Afrique, l'est de l'Asie (sauf dans l'essai d'un algorithme développé en Chine, dans lequel cas des niveaux très faibles de faux positifs parmi les images de personnes asiatiques de l'Est ont été observés), ainsi que parmi les personnes autochtones, afro-américaines, et asiatiques recherchées dans les banques de clichés anthropométriques. Les taux de faux positifs différaient en fonction de genre et d'âge, et les femmes, enfants, et personnes âgées étaient plus susceptibles à être mal identifiés.

Un système de reconnaissance faciale biaisé peut entraîner des préjudices importants, surtout envers les membres de groupes racisés déjà affectés de manière disproportionnée par la surveillance policière. En effectuant la comparaison d'images aux clichés anthropométriques d'une base de données policière, NIST a rapporté non seulement un taux élevé de faux positifs pour les personnes

afro-américaines, mais aussi un taux faible de faux négatifs, insinuant que les logiciels de reconnaissance faciale sont à la fois plus susceptibles aux mauvaises identifications et moins susceptibles à ne pas produire de correspondance.

L'arrestation arbitraire de Robert Williams à Detroit au Michigan est un exemple d'un faux positif.[62] Williams, un homme Noir, a été incorrectement signalé par un logiciel de RF comme correspondant au profil d'un criminel cherché et fut par la suite arrêté et détenu pendant 30 heures, l'identification effectuée par le système de RF étant la seule preuve.[63] Compte tenu du fait que les communautés Noires subissent un taux élevé de violence policière, un algorithme « trop désireux » de produire des identifications pour les personnes Noires est extrêmement préoccupant.

Plus de recherche est nécessaire pour déterminer où ces préjugés entrent dans les systèmes de reconnaissance faciale; il est peu clair si ces biais sont causés par la pauvre qualité des images trouvées dans les bases de données de recherche, par la composition démographique des jeux de données d'entraînement, ou par l'algorithme lui-même.

Coupable nº 1 : les caméras

Une étude menée en 2019 a démontré une forte corrélation entre la précision des algorithmes et la réflectance de la peau (ce qui a son tour correspond avec le teint de la peau, puisque les teints plus pâles reflètent plus de lumière).[64] Cependant, bien que cette corrélation persistait à travers chaque système testé, elle était nettement moins prononcée dans les systèmes avec un taux de précision général très élevé. En effet, les taux d'erreurs parmi les hommes aux teints pâles utilisant des systèmes inférieurs étaient plus élevés que les erreurs parmi les femmes aux teints plus foncés analysés avec des systèmes supérieurs. En particulier, l'étude a déduit que les différences entre les systèmes d'acquisitions (incluant la qualité des images) peuvent élargir, réduire, ou même éliminer les lacunes de précision entre les démographiques.

Coupable nº 2 : L'entraînement et les jeux de données d'essai

Pourtant, cette explication est probablement insuffisante, puisque NIST a rapporté que les taux de faux positifs pour les photographes de bonne qualité et bien éclairés demeurent différents entre les segments démographiques. De plus, la différence entre les algorithmes chinois et occidentaux à identifier correctement les visages des personnes asiatiques indique que le problème se trouve peut-être dans l'algorithme et jeux de données d'essai utilisés pour entraîner le système.

De nombreuses compagnies, incluant Clearview AI et Amazon, ne sont pas transparentes sur le sujet de la répartition démographique de leurs jeux de données d'entraînement, fait qui rend difficile l'évaluation concrète de la possibilité que le manque de diversité parmi ces jeux de données soit la cause des préjugés démographiques du système.

Des études préliminaires indiquent que ces préjugés peuvent être réduits par la création de visages artificiels utilisés pour diversifier les jeux de données d'entraînement.[65]

Coupable nº 3: L'algorithme

Cependant, d'autres études ont démontré que rectifier les jeux de données d'entraînement serait insuffisant pour contrer les préjugés sexistes, puisque les systèmes d'identification faciale « chiffrent » involontairement les renseignements sur le genre quel que soit l'équilibre de la répartition des genres dans le jeu de données d'entraînement.[66] [67] Une approche proposée est de soustraire des vecteurs de caractéristiques toute information sur le

genre, obligeant alors les algorithmes de devenir « agnostique au genre ».

Les essais

Il est également important d'examiner les jeux de données utilisés pour tester les systèmes. Bien que ces jeux de données n'affecteront pas l'exactitude d'un système, ils peuvent déformer notre évaluation de sa précision (p. ex., un algorithme avec des biais raciaux aura l'air plus exact lors d'un essai avec un jeu de données composé principalement d'images de personnes blanches). e IJB-A et Audience, deux jeux de données d'essai populaires, ont été trouvé racialement homogènes, avec respectivement 80% et 86% de leurs photos figurant des sujets aux teints pâles, ainsi représentant de façon inadéquate les personnes racisées.[68]

La plupart des systèmes de RF commerciaux utilisés par les services de police au Canada n'ont pas publié leur répartition démographique. Clearview AI, jusqu'à récemment le système le plus utilisé, n'a publié aucune information concernant la précision de leurs essais.

Le milieu de recherche sur la technologie de RF demeure maigre, comme démontré par les résultats susmentionnés variés et parfois même contradictoires. Il reste encore beaucoup à étudier et à tester avant que les systèmes de reconnaissance faciale actuellement disponibles sur le marché puissent être déclarés suffisamment exempts de partialité.

LES MORATOIRES SUR LA TECHNOLOGIE DE RF

COMMENT LES RÉGIMES RÉGULATEURS ET JURIDIQUES ACTUELS SONT INSUFFISANTS

Au Canada, le cadre juridique et les approches de la politique publique ont pris du retard sur la croissance rapide des technologies de surveillance employant la RF. Il n'existe actuellement aucune réglementation spécifique sur l'utilisation des systèmes de RF, ni de provisions spécifiques sur la collecte, l'utilisation et la conservation des données par la technologie. De plus, il n'existe aucun mécanisme indépendant pour surveiller l'utilisation de cette technologie par les services de police. Le manque de cadre régulateur clair autour des systèmes de RF risque de violer la loi sur la protection des données et de la vie privée, ce qui a encouragé les responsables politiques au Canada et ailleurs à considérer l'imposition d'un moratoire interdisant la technologie pour une durée déterminée. Les moratoires sont devenus l'outil politique par défaut des gouvernements à travers le monde lorsqu'il s'agit de réglementer l'utilisation de la RF par les services gouvernementaux et policiers. Les moratoires donnent aux législateurs et législatrices assez de temps pour développer des régimes juridiques et politiques qui peuvent assurer une utilisation responsable et sécuritaire de la RF.

INITIATIVES DU SECTEUR PRIVÉ

Au mois de juin 2020, Amazon a annoncé un moratoire de la durée d'un an sur l'utilisation policière de ses services de reconnaissance faciale.[69] IBM et Microsoft ont suivi son exemple, et IBM a cessé toutes ses activités de recherche, développement et de vente de la RF.[70] [71] Les moratoires sont apparemment prévus à fournir au Congrès américain suffisamment de temps pour développer une politique régulatrice robuste et compréhensive sur l'utilisation de la technologie de RF aux États-Unis.

INITIATIVES GOUVERNEMENTALES

Au Canada, les provisions ainsi que les cadres juridiques concernant la protection de la vie privée traînent derrière l'évolution technologique, et particulièrement celle de la reconnaissance faciale. Présentement, section 8 de la Charte canadienne des droits et libertés et les instruments internationaux tel article 12 de la Déclaration universelle des droits de l'homme éclairent la voie pour la législation protégeant la vie privée. La Loi sur la protection des renseignements personnels décrit comment protéger la vie privée en relation à la collecte, l'utilisation, et la divulgation des renseignements personnels par les institutions fédérales. La LPRPDE (Loi sur la protection des renseignements personnels et les documents électroniques), de son autre côté, traite des règlements qui s'appliquent au secteur privé. L'ambiguïté qui entoure les provisions juridiques actuelles concernant la RF est accentuée par un manque de transparence sur la manière dont la technologie est utilisée, rendant toute évaluation de sa licéité contestable. Afin de protéger les droits fondamentaux des Canadiens et Canadiennes, le gouvernement fédéral doit décider quelle est l'utilisation correcte de la technologie de RF par les institutions publiques et les forces de l'ordre. Avant de lever le moratoire, les institutions gouvernementales doivent travailler ensemble pour développer un cadre juridique robuste et des politiques claires.

L'utilisation de la technologie de RF par les services publics et policiers est interdite pour une durée de trois ans dans de nombreuses villes américaines, notamment San Francisco et Oakland.[72] En Californie actuellement, les policiers ne sont pas permis d'utiliser des caméras corporelles munis de technologie de RF.[73] De même, l'état de la Massachusetts a introduit un projet de loi établissant un moratoire sur la RF et d'autres mesures de surveillance biométriques après que Brookline et Somerville ont chacun interdit la pratique.[74] [75] Ceci suggère beaucoup de partage de connaissances politiques entre les juridictions municipales et les états. Les états du New Hampshire et de l'Oregon ont également interdit l'utilisation des caméras corporelles munies de la RF, le New Jersey a proscrit l'utilisation de la RF par les services de police, et l'état de New York a récemment suivi l'exemple en introduisant une loi interdisant toute utilisation de la technologie de RF par les services de police.[76] [77] [78] Certains états, comme le Texas et Illinois, ont exigé simplement que les compagnies obtiennent le consentement des individus avant la collecte des images faciales et tout renseignement personnel au lieu de proscrire complètement la technologie.

Au début de l'année, l'Union européenne (UE) a annoncé un plan pour un moratoire de cinq ans sur la technologie de RF. Ce moratoire fournira aux chercheurs et chercheuses plus de temps pour déterminer les pratiques les plus sûres et ainsi minimiser les « inexactitudes [qui ont le potentiel d'être] utilisées pour violer les lois protégeant les renseignements personnels et qui facilitent la usurpation de l'identité ».[79] Pourtant, depuis juin 2020, l'UE a changé de direction, et « encourage chaque état membre individuel à rédiger leurs propres lois sur la reconnaissance faciale ».[80]

Les moratoires ne sont pas le seul outil politique disponible pour améliorer la réglementation de la technologie de RF. En effet, les moratoires n'adressent pas, par essence, les enjeux fondamentaux de protection de la vie privée et des droits de la personne concernant la technologie de RF. Ils permettent plutôt aux responsables politiques un peu plus de temps pour mettre au point des standards et des lois adéquats. La plupart des moratoires sont limités, interdisant seulement certaines applications étroites de la technologie de RF

et ainsi permettant leur utilisation de manière plus élargie par la société, qui peut mener à des conséquences imprévues puisque l'utilisation se concentre dans les institutions privées. Plus important encore, il reste à savoir quand et comment les moratoires seront levés.

Une alternative politique consisterait à ajouter de contraintes supplémentaires à l'utilisation gouvernementale et policière de la RF. Au niveau fédéral aux États-Unis, le Facial Recognition Technology Warrant Act a été soumis au Congrès américain pour limiter l'utilisation de la technologie de RF par les organismes fédéraux, notamment en introduisant l'obligation d'obtenir un mandat.[81]

RÉPERCUSSIONS TECHNOLOGIQUES D'UN MORATOIRE

Toute proposition d'un moratoire devrait clairement établir quelles technologies spécifiques peuvent et ne peuvent pas être utilisées et à quelle fin, ainsi pour quels organismes gouvernementaux l'utilisation sera proscrite. Par exemple, un moratoire qui interdit l'utilisation de la technologie de RF par les services policiers n'interdirait pas nécessairement la police à obtenir et à effectuer des essais avec la technologie. De plus, puisque la plupart des services de police agissent au niveau provincial/territorial ou au niveau local, un moratoire fédéral n'affecterait pas directement la plupart des activités policières. Une provision pourrait à la place être incluse pour limiter le financement fédéral si les provinces et les villes n'appliquent pas leurs propres moratoires.

Un exemple potentiel de moratoire fédéral est le Facial Recognition and Biometric Technology Moratorium Act of 2020, récemment introduit au Sénat américain.[82] Les systèmes informatiques biométriques comprennent non seulement la technologie de RF mais sont définis de manière plus élargie comme étant toute technologie qui capture ou déduit des renseignements sur une personne, notamment son identité, ses émotions, ou sa location, à partir de leurs visages, leurs voix, leurs allures, ou autres caractéristiques.

Si l'acte est adopté, il interdira l'achat, l'utilisation, ou la collecte indirecte (par des tiers) de toute information obtenue par un système biométrique (excluant la reconnaissance d'empreintes digitales) par les organismes fédéraux. Les organismes qui violent la loi pourront être assujettis par des poursuites civiles lancées par des individus ou des procureurs généraux des états. Les organismes locaux ou de l'état ne pourront recevoir de financement fédéral important s'ils n'adoptent pas des mesures ou lois similaires. L'Institut national américain des normes et de la technologie (NIST) continuera d'avoir la permission d'essayer et de rechercher la technologie de RF, et des utilisations particulières de la technologie pourront être autorisées par le Congrès un jour. Cette autorisation future devra non seulement définir qui peut utiliser quelle technologie et à quelle fin, mais aussi établir les exigences des vérifications, les standards de conservation et d'utilisation des données, et les seuils de précision démographique minimum.

Une application de ce cadre au contexte canadien inclura la proscription spécifique de l'utilisation d'un service de RF par la GRC, qu'il soit acheté ou non. L'interdiction pourrait aussi s'étendre pour s'appliquer à l'ASFC. Les gouvernements provinciaux seront

alors encouragés à introduire leurs propres moratoires, suivant l'exemple du gouvernement fédéral, en limitant l'utilisation de la technologie de RF par leurs propres services de police et autres organismes provinciaux. La limitation des services de RF pourrait également s'étendre aux sociétés d'État, les entreprises gouvernementales, et l'utilisation par le secteur privé.

PROCHAINES ÉTAPES

Un moratoire n'est pas une solution permanente. Plutôt, il sert à donner aux responsables politiques assez de temps pour mener les études et évaluation nécessaires de la technologie de reconnaissance faciale et estimer méticuleusement ses conséquences pour ensuite développer un cadre politique robuste pour réguler la RF. La deuxième document de cette série, Exposé n° 2, se concentre sur les conditions technologiques, sociales, et politiques requises pour lever un moratoire fédéral.

RÉFÉRENCES

1 Weise, Karen, et Natasha Singer. “Amazon Pauses Police Use of Its Facial Recognition Software.” The New York Times, 10 juin 2020. https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html.

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

3 Taylor Owen et 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, 14 février 2020. https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/.

4 “Amazon Rekognition FAQs.” Amazon Web Services. Amazon. Accessed July 8, 2020. https://aws.amazon.com/rekognition/faqs/.

5 Partnership on AI. “Understanding Facial Recognition Systems.” February 19, 2020. https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf.

6 “Your Privacy at Airports and Borders.” Office of the Privacy Commissioner of Canada, December 17, 2018. https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/your-privacy-at-airports-and-borders/.

7 Ibid.

8 “BorderXpress™.” Innovative Travel Solutions. Accessed July 8, 2020. https://www.innovativetravelsolutions.ca/products/borderxpress/.

9 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.

10 Kate Allen, Wendy Gillis, and Alex Boutilier. “Facial Recognition App Clearview AI Has Been Used Far More Widely in Canada than Previously Known.” Toronto Star, February 28, 2020. https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html.

11 “Facial Recognition To Aid Investigations.” The City of Calgary Newsroom. City of Calgary, November 3, 2014. https://newsroom.calgary.ca/facial-recognition-to-aid-investigations/.

12 David Burke. “Privacy Laws Lag behind as Some Canadian Police Forces Begin to Use Facial Recognition Technology.” CBC News. CBC, February 10, 2020. https://www.cbc.ca/news/canada/nova-scotia/facial-recognition-police-privacy-laws-1.5452749.

13 Bryann Aguilar. “Toronto Police Chief Unaware Officers Have Been Using Controversial Facial Recognition Software for Months.” CTV News, February 14, 2020. https://toronto.ctvnews.ca/toronto-police-chief-unaware-officers-have-been-using-controversial-facial-recognition-software-for-months-1.4811434.

14 “RCMP Use of Facial Recognition Technology.” Royal Canadian Mounted Police, February 27, 2020. https://www.rcmp-grc.gc.ca/en/news/2020/rcmp-use-facial-recognition-technology.

15 Ibid.

16 Ibid.

17 Catharine Tunney. “RCMP Says It Will Limit Its Use of Facial Recognition Tech—but Won’t Stop Using It Entirely.” CBC News. CBC, March 23, 2020. https://www.cbc.ca/news/politics/rcmp-clearview-ai-1.5490988.

18 Research Group of the Office of the Privacy Commissioner of Canada. “Automated Facial Recognition in the Public and Private Sectors” March 2013. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/.

19 Ibid.

20 Chris Frey. “Revealed: How Facial Recognition Has Invaded Shops – and Your Privacy.” The Guardian, March 3, 2016. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.

21 “From facial recognition to extra staff: High and low tech tools used to combat shoplifting in Winnipeg.” CTV News, February 21, 2019. https://winnipeg.ctvnews.ca/from-facial-recognition-to-extra-staff-high-and-low-tech-tools-used-to-combat-shoplifting-in-winnipeg-1.4307648.

22 Marie-Claude Malboeuf. “Bell veut vous faire suivre en continu.” La Presse, February 27, 2020. https://www.lapresse.ca/actualites/2020-02-27/bell-veut-vous-faire-suivre-en-continu.

23 “Amazon Rekognition.” Amazon Web Services, Amazon, Accessed July 8, 2020. https://aws.amazon.com/rekognition/?blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc.

24 Jason Del Rey. “Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers.” Vox, September 26, 2019. https://www.vox.com/recode/2019/9/25/20884427/jeff-bezos-amazon-facial-recognition-draft-legislation-regulation-rekognition.

25 Karen Weise and Natasha Singer. “Amazon Pauses Police Use of Its Facial Recognition Software.” The New York Times, June 10, 2020. https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html.

26 “First Report of the Axon AI & Policing Technology Ethics Board.” The Policing Project. Accessed July 8, 2020. https://www.policingproject.org/axon-fr.

27 Kate Allen, Wendy Gillis, and Alex Boutilier. “Facial Recognition App Clearview AI Has Been Used Far More Widely in Canada than Previously Known.” Toronto Star, February 28, 2020. https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html.

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

29 Kashmir Hill. “The Secretive Company That Might End Privacy as We Know It.” The New York Times, January 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

30 Rebecca Heilwiel. “The world’s scariest facial recognition company, explained.” Vox, May 8, 2020. https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

31 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.

32 Yaniv Taigman, Ming Yang, Marc Aurelio Ranzato, and Lior Wolf.” DeepFace: Closing the Gap to Human-Level Performance in Face Verification.” (paper presented at the Conference on Computer Vision and Pattern Recognition, Greater Columbus Convention Center, Columbus, Ohio, June 24, 2014), https://research.fb.com/wp-content/uploads/2016/11/deepface-closing-the-gap-to-human-level-performance-in-face-verification.pdf.

33 Ibid.

34 Sigel Samuel. “Facebook will finally ask permission before using facial recognition on you.” Vox, September 4, 2019. https://www.vox.com/future-perfect/2019/9/4/20849307/facebook-facial-recognition-privacy-zuckerberg.

35 Lesley Fair. “FTC’s $5 billion Facebook settlement: Record-breaking and history-making.” Federal Trade Commission, July 24, 2019. https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

36 “Unlock your Pixel phone with your face.” Pixel Phone Help. Google. Accessed July 8, 2020. https://support.google.com/pixelphone/answer/9517039?hl=en.

37 “Search by people, things & places in your photos.” Google Photos Help. Google. Accessed July 8, 2020. https://support.google.com/photos/answer/6128838?co=GENIE.Platform%3DAndroid&hl=en.

38 “Detect faces.” Google Cloud. Google. Accessed July 8, 2020. https://cloud.google.com/vision/docs/detecting-faces.

39 “How Google uses pattern recognition to make sense of images.” Google. Accessed July 8, 2020. https://policies.google.com/technologies/pattern-recognition?hl=en-US.

40 Julia Carrie Wong. “Google reportedly targeted people with ‘dark skin’ to improve facial recognition.” The Guardian, October 3, 2019. https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color.

41 Jennifer Elias. “Google employees petition company to cancel police contracts.” CNBC, June 22, 2020. https://www.cnbc.com/2020/06/22/google-employees-petition-company-to-cancel-police-contracts.html.

42 Dave Gershgorn. “A Single Company Will Now Operate Facial Recognition for Nearly 800 Million People.” OneZero, June 5, 2020. https://onezero.medium.com/idemia-will-operate-facial-recognition-for-nearly-800-million-people-69b72582202b.

43 “Public security & law enforcement.” IDEMIA. Accessed July 8, 2020. https://www.idemia.com/public-security-law-enforcement.

44 “General Data Protection Regulation.” Intersoft Consulting. Accessed July 8, 2020. https://gdpr-info.eu/.

45 Tristan Péloquin. “Reconnaissance faciale: la SQ pourrait acquérir une technologie controversée.” La Presse, June 22, 2020. https://www.lapresse.ca/actualites/justice-et-faits-divers/2020-06-22/reconnaissance-faciale-la-sq-pourrait-acquerir-une-technologie-controversee.

46 “Face.” Microsoft Azure. Microsoft. Accessed July 8, 2020. https://azure.microsoft.com/en-ca/services/cognitive-services/face/#overview.

47 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.

48 “OPS tested facial recognition software, but doesn’t use it.” CBC News. CBC, February 15, 2020. https://www.cbc.ca/news/canada/ottawa/ottawa-police-facial-recognition-1.5464964.

49 “Third-Party Authenticated.” NEC. Accessed July 8, 2020. https://www.necam.com/AdvancedRecognitionSystems/NISTValidation/FingerprintFacial/.

50 NEC, Advanced Criminal Investigative Solution Using Face Recognition Technology: NeoFace® Reveal, Irving, Texas, 2017. https://www.necam.com/Docs/?id=e838a769-4fa5-4264-bd1c-d9eeedf7b527.

51 "Bio-IDiom." NEC. Accessed July 8, 2020. https://www.nec.com/en/global/solutions/biometrics/index.html.

52 Louise Matsakis. "Scraping the Web Is a Powerful Tool. Clearview AI Abused It." Wired. January 25, 2020. https://www.wired.com/story/clearview-ai-scraping-web/.

53 Jon Porter. "Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech." The Verge. February 6, 2020. https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube.

54 Kashmir Hill. "Twitter Tells Facial Recognition Trailblazer to Stop Using Photos." The New York Times. January 22, 2020. https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.

55 Nick Statt. "ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy" The Verge. May 28, 2020. https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws.

56 Identity Theft Resource Center (ITRC). "2019 End of Year Data Breach Report." Identity Theft Resource Center, January 28, 2020. https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

57 Bryann Aguilar. "Company behind controversial facial recognition software used by Toronto police suffers data breach." CTV News, February 26, 2020. https://toronto.ctvnews.ca/company-behind-controversial-facial-recognition-software-used-by-toronto-police-suffers-data-breach-1.4829200.

58 Josh Taylor. "Major breach found in biometrics system used by banks, UK police and defence firms." The Guardian, August 14, 2019. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms?CMP=share_btn_tw.

59 Ibid.

60 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.

61 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).

62 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.

63 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.

64 Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton, and Arun R. Vemury. "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," IEEE Transactions on Biometrics, Behavior, and Identity Science, 1, no. 1 (2019), 32-41, http://jjhoward.org/wp-content/uploads/2019/02/demographic-effects-image-acquisition.pdf (accessed July 8, 2020).

65 Adam Kortylewski et al. "Analyzing and Reducing the Damage of Dataset Bias to Face Recognition with Synthetic Data" (paper presented at the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, June 16-20, 2019), 2261-2268. https://openaccess.thecvf.com/content_CVPRW_2019/papers/BEFA/Kortylewski_Analyzing_and_Reducing_the_Damage_of_Dataset_Bias_to_Face_CVPRW_2019_paper.pdf.

66 Prithviraj Dhar, Joshua Gleason, Hossein Souri, Carlos D. Castillo, and Rama Chellappa. "An adversarial learning algorithm for mitigating gender bias in face recognition." June 14, 2020. https://arxiv.org/pdf/2006.07845.pdf.

67 Tianlu Wang, Jieyu Zhao, Mark Yatskar, Kai-Wei Chang, and Vicente Ordonez. "Balanced Datasets Are Not Enough: Estimating and Mitigating Gender Bias in Deep Image Representations" (paper presented at the 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, South Korea, October 27-November 2, 2019), 5309-5318. https://arxiv.org/pdf/1811.08489.pdf (accessed July 8, 2020).

68 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.

69 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.

70 Jay Peters. "IBM will no longer offer, develop, or research facial recognition technology." The Verge, June 8, 2020. https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software.

71 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/.

72 Kate Conger, Richard Fausset and Serge F. Kovaleski. “San Francisco Bans Facial Recognition Technology.” The New York Times, May 14, 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

73 Rachel Mentz. “California lawmakers ban facial-recognition software from police body cams.” CNN Business. CNN, September 13, 2019. https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html.

74 Bill S.1385. “An Act establishing a moratorium on face recognition and other remote biometric surveillance systems.” Commonwealth of Massachusetts. https://malegislature.gov/Bills/191/S1385.

75 Nik DeCosta-Klipa. “Brookline becomes 2nd Massachusetts community to ban facial recognition.” Boston.com. December 12, 2019. https://www.boston.com/news/local-news/2019/12/12/brookline-facial-recognition.

76 ACLU NorCal. “California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams.” October 8, 2019. https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams.

77 Max Read. “Why We Should Ban Facial Recognition Technology.” Intelligencer. January 30, 2020. https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html.

78 Jane Wester. “NY State Senate Bill Would Ban Police Use of Facial Recognition Technology.” Law.com. January 27, 2020. https://www.law.com/newyorklawjournal/2020/01/27/ny-state-senate-bill-would-ban-police-use-of-facial-recognition-technology/?slreturn=20200608172543.

79 Javier Espinoza and Madhumita Murgia. “EU backs away from call for blanket ban on facial recognition tech.” Financial Times, February 11, 2020. https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5

80 Christine Fisher. ‘EU backs away form proposed five year facial recognition ban.’ Engadget, February 11, 2020. https://www.engadget.com/2020-02-11-european-commission-facial-recognition-guidelines.html

81 ALB19A70. “A Bill to limit the use of facial recognition technology by Federal agencies, and for other purposes.” https://www.coons.senate.gov/imo/media/doc/ALB19A70.pdf.

82 Ibid.