Mondialisation.ca
Centre de recherche sur la mondialisation

Plus qu'effrayant : la sécurité intérieure cherche à partager les banques de données biométriques avec des pays étrangers

Par Children's Health Defense
Mondialisation.ca, 16 août 2022
The Defender 11 août 2022

Thème: Droits humains et État policier, Science et médecine, Services de renseignements
Analyses: COVID-19

Selon un rapport de Statewatch du 22 juillet, le ministère américain de la sécurité intérieure (DHS) encourage les "accords de sécurité frontalière renforcée" en offrant un accès aux vastes banques de données biométriques du ministère aux États étrangers qui acceptent de rendre la pareille.

Un document du DHS, intitulé "DHS International Biometric Information Sharing (IBIS) Program", est en fait un "argumentaire de vente" destiné à des "partenaires étrangers" potentiels, selon Statewatch.

Selon le document, le programme IBIS fournit "une capacité bilatérale évolutive, fiable et rapide de partage d'informations biométriques et biographiques pour soutenir la sécurité des frontières et le contrôle de l'immigration".

Les technologies biométriques fonctionnent en identifiant des caractéristiques uniques dans les traits biologiques d'une personne et en les comparant à des informations stockées pour voir si une personne est bien celle qu'elle prétend être.

Selon le DHS, ces caractéristiques, qui peuvent être physiques, telles qu'une empreinte digitale ou un dessin d'iris, ou comportementales, telles que des modèles vocaux, sont utilisées pour la "reconnaissance automatisée" des individus.

Certains défenseurs des libertés civiles et des droits de l'homme ont exprimé des inquiétudes quant à la collecte d'informations biométriques par le DHS, les gouvernements étrangers et les entreprises.

"Ce n'est pas seulement la surveillance et l'achat et la vente de vos données qui sont inquiétants", a déclaré à The Defender John Whitehead, avocat spécialisé dans les libertés civiles et auteur.

"Les ramifications d'un gouvernement, quel qu'il soit, disposant d'autant de pouvoir non réglementé et non responsable pour cibler, suivre, rassembler et détenir ses citoyens sont plus que terrifiantes", a-t-il déclaré.

L'utilisation croissante des technologies biométriques est une question d'argent et de profits, a déclaré M. Whitehead.

Il ajoute:

“Nous avons été réduits à des bits de données et à des unités économiques à acheter, à troquer et à vendre au plus offrant, par le gouvernement et des entreprises américaines.

“Cette nouvelle ère effrayante d’espionnage gouvernemental/entreprise, dans laquelle nous sommes écoutés, surveillés, suivis, cartographiés, achetés, vendus et ciblés, fait paraître la surveillance de la NSA [Agence nationale de sécurité des États-Unis] presque désuète en comparaison.”

La surveillance étendue des citoyens américains, révélée pour la première fois par l’ancien contractant de la NSA Edward Snowden en 2013, et qui a fait l’objet d’un procès par le syndicat américain des libertés civiles (American Civil Liberties Union, ou ACLU), fonctionne toujours sans contrôle judiciaire et avec un contrôle limité du Congrès, selon un rapport publié en juin 2021 dans le Washington Post.

Bien que la surveillance continue des citoyens par la NSA soit problématique, M. Whitehead a déclaré qu’il était plus préoccupé par le “panopticon”génétique d’aujourd’hui – une prison numérique de surveillance constante – dans lequel “nous sommes tous des suspects dans une séance d’identification génétique, attendant d’être associés à un crime”.

“À l’ère de la criminalisation à outrance, de la surveillance 24 heures sur 24 et d’un État policier désireux de montrer ses muscles, nous sommes tous coupables d’une transgression ou d’une autre”, écrit Whitehead dans un article publié le 27 juillet par l’Institut Rutherford.

Nous sommes surveillés jusque dans nos gènes.

Les entreprises et les gouvernements du monde entier investissent rapidement dans les nouvelles technologies d’identification et de suivi des personnes, selon Global Newswire, qui a estimé en juin que le marché représentera près de 49 milliards de dollars en 2022 et prévoit qu’il fera plus que doubler, pour atteindre 102 milliards de dollars, d’ici 2027.

Le marché mondial de l’identification humaine, qui comprend les technologies biométriques de l’ADN utilisées pour la médecine légale, les tests de paternité et “d’autres applications“, devrait atteindre 6 435,6 millions de dollars d’ici 2032, soit plus de quatre fois et demie les bénéfices du secteur en 2021, a rapporté Global News Wire le mois dernier.

Le rapport de 231 pages publié le mois dernier sur ReportLinker met en évidence les tendances dominantes du marché de l’identification humaine et les facteurs de croissance du marché, notamment la demande croissante de produits et de technologies d’identification humaine.

Commentant l’utilisation prolifique des technologies biométriques, M. Whitehead a déclaré :

“Nous sommes surveillés jusque dans nos gènes, grâce à une puissante combinaison de matériel, de logiciels et de collecte de données qui scanne nos données biométriques : notre visage, notre iris, notre voix, notre génétique et même notre démarche, les soumet à des programmes informatiques capables de décomposer les données en “identifiants” uniques, puis les offre au gouvernement et à ses alliés commerciaux pour leurs usages respectifs.”

Selon Whitehead, le système actuel de capitalisme de surveillance à but lucratif qui menace la vie privée des gens est rendu possible par la coopération des individus.

Toutes les clauses de non-responsabilité que vous faites défiler sans les lire, celles qui sont écrites dans une police de caractères minuscule, pour cliquer rapidement sur le bouton "Accepter" à la fin afin de pouvoir passer à l'étape suivante – télécharger un logiciel, ouvrir un compte de média social, ajouter une nouvelle application à votre téléphone ou à votre ordinateur – signifient votre consentement écrit à ce que vos activités soient surveillées, enregistrées et partagées", a déclaré M. Whitehead.

Il a également fait remarquer que "chaque geste que vous faites" en ligne est "surveillé, extrait des données, analysé et compilé" afin que les spécialistes du marketing puissent se faire une idée de qui vous êtes, de ce qui vous fait tiquer et de la meilleure façon de vous influencer et/ou de vous contrôler.

Whitehead a déclaré :

"Avec chaque smartphone que nous achetons, chaque dispositif GPS que nous installons, chaque Twitter, Facebook et Google que nous ouvrons, chaque carte d'acheteur fréquent que nous utilisons pour nos achats – que ce soit à l'épicerie, au magasin de yaourt, à la compagnie aérienne ou au grand magasin – et chaque carte de crédit et de débit que nous utilisons pour payer nos transactions, nous aidons les entreprises américaines à constituer un dossier pour leurs homologues gouvernementaux sur qui nous savons, ce que nous pensons, comment nous dépensons notre argent et comment nous passons notre temps."

Selon M. Whitehead, chaque jour, l'Américain moyen qui vaque à ses occupations sera surveillé, épié et suivi de plus de 20 façons différentes par les yeux et les oreilles du gouvernement et des entreprises.

Il a ajouté :

"La technologie a tellement progressé que les spécialistes du marketing (les campagnes politiques sont parmi les pires contrevenants) peuvent en fait construire des "clôtures numériques" autour de vos maisons, de vos lieux de travail, des maisons de vos amis et de votre famille et d'autres lieux que vous visitez afin de vous bombarder de messages spécialement conçus pour obtenir un résultat particulier."

Selon M. Whitehead, le niveau de transgression de la vie privée des individus par les entreprises est si envahissant que si les auteurs étaient des harceleurs individuels, les victimes pourraient appeler la police.

Mais cela ne serait pas efficace dans cette situation, a-t-il dit, car les services policiers américains sont fréquemment impliqués dans la surveillance biométrique.

Whitehead a déclaré :

"Si quelqu'un d'autre nous traquait de cette manière – en nous suivant partout où nous allons, en écoutant nos appels, en lisant notre correspondance, en découvrant nos secrets, en nous profilant et en nous ciblant en fonction de nos intérêts et de nos activités – nous appellerions les flics."

"Malheureusement, les flics (équipés de dispositifs Stingray et d'autres technologies de voyeurisme) sont également dans le coup pour cette arnaque particulière."

L'utilisation de la reconnaissance faciale par la police a "à juste titre" mauvaise presse.

Une partie de la confusion et de la controverse que suscite le discours public sur la biométrie tient au fait qu'il existe de multiples utilisations d'une même technologie, a déclaré Michael Magrath, consultant de haut niveau sur l'identité numérique et défenseur de la vie privée et de la sécurité.

M. Magrath a déclaré au Defender que la technologie de reconnaissance faciale, en particulier, est utilisée de diverses manières et que ces manières devraient être évaluées séparément.

M. Magrath est directeur général de la pratique de l'identité numérique pour la société de conseil Kuma – une entreprise mondiale spécialisée dans la protection de la vie privée, la sécurité et l'identité, qui propose des solutions personnalisées de cybersécurité.

Selon un communiqué de presse du 27 juin, Kuma est le premier et le seul évaluateur au monde à proposer des certifications d'identité numérique pour les États-Unis et le Canada.

"Nous devons délimiter les cas d'utilisation qui font appel à la reconnaissance faciale", a déclaré M. Magrath. "J'aime les considérer comme deux cas d'utilisation différents".

Selon M. Magrath, l'utilisation des technologies de reconnaissance faciale par les forces de l'ordre "a vraiment mauvaise presse et, à mon avis, à juste titre".

M. Magrath s'est dit opposé à l'installation de "caméras tout autour" des villes, qui filment les gens et utilisent la technologie de reconnaissance faciale sans leur consentement. "Je ne suis pas du tout d'accord avec cela", a-t-il déclaré.

Ted Claypoole, expert juridique et président du comité du cyberespace de l'American Bar Association, a également signalé cette utilisation de la technologie de reconnaissance faciale en raison de la façon dont elle menace le droit à la vie privée des personnes.

Claypoole, qui a récemment co-écrit le livre "Privacy in the Age of Big Data : Recognizing Threats, Defending Your Rights, and Protecting Your Family", a déclaré au Defender que les problèmes de confidentialité apparaissent lorsque les données biométriques du visage capturées par des caméras vidéo sont soumises à des programmes de reconnaissance par intelligence artificielle (IA).

"Soudainement", a déclaré Claypoole, "les utilisateurs de ces systèmes peuvent identifier par leur nom chaque personne qui est passée par une intersection un jour ou qui est entrée dans une clinique de santé pour femmes."

"Il y a une partie importante de nos vies modernes qui s'appelle la vie privée par l'obscurité", a-t-il déclaré.

Claypoole a dit :

"Si vous êtes assis dans un parc bondé, vous ne vous attendez pas à ce que tout le monde sache qui vous êtes. Si vous le faisiez, cela inhiberait votre comportement. Ainsi, lorsque la police peut utiliser des systèmes de reconnaissance faciale pour scanner et identifier chaque participant à une manifestation politique pacifique, cette obscurité est menacée, tout comme votre droit de libre association garanti par le premier amendement, qui peut s'appuyer sur l'obscurité dans certaines circonstances.

“Si les personnes qui peuvent menacer votre vie privée, comme la police, Facebook, votre patron ou votre belle-mère, ont la capacité de surveiller certaines zones et d’identifier les personnes qui y apparaissent, alors vous avez perdu une importante liberté de mouvement et d’association dans votre vie.”

Magrath et Claypoole ont déclaré qu’ils trouvaient cette utilisation de la reconnaissance faciale inquiétante.

M. Magrath a également fait remarquer que cette technologie est très différente de la technologie biométrique qui utilise les données faciales pour se connecter à un appareil personnel, tel qu’un téléphone.

M. Magrath a déclaré qu’il qualifierait l’utilisation par l’IA des données faciales pour se connecter à un téléphone ou à un ordinateur de “faire correspondre des visages plutôt que de les reconnaître “.

Il a dit :

“Idéalement, la biométrie est stockée en toute sécurité dans l’appareil et ne part pas dans un grand entrepôt de données dans le ciel.

” La correspondance se ferait sur l’appareil. L’algorithme déterminera que l’empreinte digitale ou le visage est le mien, et je pourrai me connecter à un site web ou à mon téléphone, par exemple.

“Cela se fait sur l’appareil, et c’est très sécurisé”.

L’ACLU exhorte les citoyens à évaluer de manière critique les différents types de technologies biométriques et la façon dont elles sont utilisées, en particulier lorsque les forces de police de leur communauté souhaitent mettre en œuvre une nouvelle technologie de surveillance.

Six questions à poser avant d’accepter une technologie de surveillance

Jay Stanely, analyste politique principal pour le projet Speech, Privacy, and Technology de l’ACLU, a écrit le mois dernier :

“Si la police de votre communauté déclare vouloir installer une nouvelle technologie de surveillance, telles que reconnaissance faciale, caméras ou scanners de plaques d’immatriculation, par exemple, il est probable qu’elle sera présentée comme le moyen de prévenir toutes sortes de maux, du terrorisme à la criminalité de rue en passant par la fraude et le vol de colis.

“Si nous enregistrons tout, à en croire les partisans de la surveillance, nous pourrons arrêter ou résoudre des crimes et la vie sera meilleure.

“Les autorités auront probablement aussi des histoires spécifiques à vous raconter – hypothétiques ou réelles – dans lesquelles la technologie a sauvé la mise.

“Comment devrions-nous traiter ces demandes ? Si la technologie peut faire du bien, devons-nous l’accepter ?”

Selon M. Stanely, les citoyens devraient se poser ces questions avant d'accepter une technologie de surveillance :

1. La technologie fonctionne-t-elle ?
2. Quelle est l'efficacité de la technologie ?
3. Quelle est l'importance du danger que la technologie est censée réduire ?
4. Quels sont les effets secondaires négatifs de cette technologie ?
5. Quels sont les coûts d'opportunité liés à la dépense de ressources pour cette technologie ?
6. La communauté la veut-elle ?

Les technologies de surveillance doivent être soumises à l'examen du public, a souligné M. Stanely, car "les effets secondaires de la surveillance peuvent inclure la perte de la vie privée, la possibilité d'abus, nuire à la créativité et à la liberté d'expression, et avoir des impacts raciaux disparates qui aggravent les injustices sociales existantes".

La source originale de cet article est The Defender

Articles Par : Children's Health Defense