

La cybersécurité des applications de notification des contacts

Mémoire présenté dans le cadre des auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19.

14 août 2020

09h00

Hôtel du Parlement

Claude Sarrazin

Président

SIRCO enquête et protection

3905, Boulevard Industriel

Montréal (Québec) H1H2Z2

Présentation du spécialiste en cybersécurité

Président-fondateur de SIRCO, Claude A. Sarrazin œuvre dans le domaine de la sécurité privée et publique depuis 1987. Il est renommé pour ses qualités de communicateurs et ses compétences professionnelles. C'est d'ailleurs un conférencier recherché qui s'implique également comme enseignant et formateur dans plusieurs formations universitaires reliées au monde de l'enquête à la Faculté de Criminologie de l'Université de Montréal et à l'école des Sciences de la Gestion de l'UQAM où il enseigne en cybercriminalité.

Gestionnaire ambitieux ayant plus de 30 ans d'expérience pertinente au sein d'organisations majeures, Claude Sarrazin est reconnu comme étant un conseiller stratégique efficace par plusieurs conseils d'administration et gouvernement. Ses connaissances approfondies des secteurs de la sécurité privée et publique lui permettent d'amener une nouvelle perspective sur les enjeux contemporains touchant la société québécoise.

En plus d'avoir été enquêteur chef pour le Tribunal Pénal International, monsieur Sarrazin a souvent dirigé des enquêtes complexes, tant au Canada qu'à l'international. Monsieur Sarrazin a également collaboré à des dossiers de fraude et de contrefaçon à l'échelle mondiale. Devant l'émergence de nouvelles technologies de l'information, M. Sarrazin a su innover et se faire une place parmi les précurseurs en matière de solutions de crimes informatiques. D'ailleurs, SIRCO a été la première firme canadienne à mener à terme une enquête informatique résultant à un dépôt d'accusations criminelles.

Depuis 2005, Claude Sarrazin œuvre à titre d'expert auprès de plusieurs médias (*Groupe TVA, COGECO Radio, CTV*) pour des questions touchant la sécurité et la police. De plus, il siège au comité de discipline et déontologie policière et agit à titre de formateur auprès du Barreau du Québec. Il siège également à de nombreux conseils d'administration. Il est vice-président du conseil d'administration du CIPC (Centre international de prévention du crime) une ONG internationale en matière de prévention du crime dont les crimes technologiques.

Résumé

Différents types d'applications de suivis de contacts et de localisation ont été utilisés dans plusieurs pays. Certaines applications sont utilisées pour assurer la quarantaine alors que d'autres sont utilisées pour détecter les contacts entre les personnes atteinte de COVID-19 et les personnes saines.

Lorsqu'on envisage l'utilisation d'applications de notification ou de suivi de contacts, il est important de noter toutes les implications. Les applications utilisant la technologie GPS sont plus intrusives que celles qui utilisent uniquement la technologie Bluetooth et posent plus de risques quant à la cybersécurité. Afin d'accroître la sécurité des données personnelles et de protéger la confidentialité et le droit à la vie privée, seule la technologie Bluetooth doit être utilisée. Aucune donnée ne doit être collectée ou analysée dans des serveurs centralisés, toutes les analyses doivent être effectuées directement sur le téléphone de l'utilisateur.

Exposé général

En prémisses, nous aimerions mentionner que le suivi des contacts pour les personnes porteuses de virus est une méthode reconnue dans le passé pour d'autres pandémies telles que celles occasionnées par le virus du A H1N1 et de l'Ebola.^{1,2} Alors pourquoi ne pas utiliser des moyens technologiques qui se trouvent à notre portée et dignes du deuxième millénaire ? Nous allons donc souligner ce qui se fait actuellement et présenter les risques de cette nouvelle pratique.

Les applications de suivi de contacts permettent de notifier les gens qui présente un risque accru d'avoir contracté le SARS-CoV-2 grâce à la proximité entre deux appareils numériques. Cette notification a pour but d'encourager rapidement l'utilisateur à se faire tester pour la COVID-19 et à s'isoler de façon à ne pas propager le virus, même en l'absence de symptômes. De plus, l'organisation mondiale de la santé indique que les données recueillies grâce à l'utilisation d'applications de suivi de contacts pourraient aider les chercheurs à mieux se préparer pour d'autres vagues de COVID-19 ou pour de futures pandémies.³

Le *contact tracing* est une partie importante de la stratégie (avec les tests) pour éliminer et contrôler la propagation du Covid-19. Cette application permet à une personne ayant testé positif (en suivant ses instructions) de déclarer son état de façon à prévenir anonymement les personnes ayant été à proximité et de prévenir cette même personne si elle a été en contact avec une personne atteinte de la Covid-19. Le fait de recueillir les données personnelles d'individus poserait ici un problème quant à la protection de la vie privée s'il n'y a pas de sécurité suffisante et de surveillance indépendante appropriée de l'utilisation des données recueillies. Qui a vraiment accès à ces données ? ⁴

1 World Health Organization, (2015, July 23). Contact tracing, Retrieved from <https://www.who.int/csr/disease/ebola/training/contact-tracing/en/>

2 Swaan, Corien M.; Appels, Rolf; Kretzschmar, Mirjam E. E.; van Steenbergen, Jim E. (2011-12-28). "Timeliness of contact tracing among flight passengers for influenza A/H1N1 2009". *BMC Infectious Diseases*. **11** (1): 355. doi:10.1186/1471-2334-11-355.

3 Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Interim Guidance. World Health Organization. 05/28/20

⁴ <https://globalnews.ca/news/7080914/coronavirus-ontario-covid-19-tracing-app/>

Ces applications exigent une participation volontaire d'une majeure partie de la population afin d'être efficaces. Il est donc primordial de ne pas faire d'erreur puisque ça pourrait compromettre les résultats désirés si les citoyens perdent confiance en leur gouvernement et refusent d'utiliser une application de suivi de contacts.⁵ C'est pourquoi Google et Apple ont annoncé en avril qu'ils travailleraient de concert à développer une application qui serait bâtie de façon à prioriser la confidentialité et la sécurité afin de permettre aux gouvernements et aux agences de santé publique d'utiliser celle-ci.⁶ Un associé de recherche principal au Citizen Lab, de l'Université de Toronto, Christopher Parsons, mentionne un seuil de 65% à 80% d'utilisation de l'application pour que celle-ci ait un impact majeur sur la propagation du virus.⁷ Cependant, il faut prendre en compte que ce n'est pas 100% de la population qui possède un téléphone intelligent donc afin d'obtenir un seuil d'utilisation de près de 60% de la population il faut qu'une grande majorité des utilisateurs de téléphones intelligents utilise l'application de notification de contacts. Une étude démontre qu'en Islande, l'utilisation d'une application de notification de contacts, avec un taux d'utilisation près de 40%, n'a eu que très peu d'effets sur le ralentissement de la propagation du virus.⁸

En effet, il n'y a aucune étude empirique indiquant qu'une application de suivi de contacts serait efficace pour lutter contre la pandémie si ce n'est pas la grande majorité de la population qui l'utilise. Il pourrait s'avérer difficile de convaincre suffisamment de citoyens étant donné les scandales de fuites de données, autant au public qu'au privé, dans les dernières années.⁹

Plusieurs experts en cybersécurité et en confidentialité croient que l'utilisation d'applications de suivi de contacts peut devenir rapidement problématique et qu'il pourrait être difficile par la suite de reculer sur leur utilisation. Amnistie Internationale mentionne que les leçons que l'on peut tirer

⁵ <https://www.droit-inc.com/article27155-6-questions-a-Me-Gratton-sur-l-application-Alerte-COVID>

⁶ <https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf>

⁷ <https://www.lapresse.ca/covid-19/2020-08-03/les-problemes-d-accessibilite-de-l-application-alerte-covid-critiques.php>

⁸ <https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/>

⁹ *A Scramble for Virus Apps That Do No Harm. New York Times 06/03/20*

<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

de l'histoire récente, comme le 11 septembre 2001, sont que les outils de surveillance développés et utilisés en temps de crise sont rarement abandonnés une fois la crise passée. C'est pourquoi les outils utilisés devraient être le moins envahissant et intrusif possible. Les gouvernements ne devraient pas avoir accès aux données personnelles de membres de la population.¹⁰ De plus, Dr. Woodrow Hartzog professeur de droit et science informatique à Northeastern University a indiqué les conséquences qui pourraient s'en suivre de cette façon : "We've already learned what moving fast and breaking things can do to society," en référence aux mesures mises en place après les attentats du 11 septembre 2001.¹¹

Par contre, il est vrai que d'utiliser une application de suivi de contacts pourrait permettre de concentrer les efforts de suivi de contacts traditionnel sur les personnes qui n'ont pas accès à ce type de technologies comme les personnes âgées et moins fortunées. Celles-ci sont généralement plus vulnérables.¹²

Pourtant Apple et Google indiquent en ce qui a trait aux **Exposures Notifications** pour **Bluetooth Specification** et **Cryptography Specification** le message suivant: *Preliminary — Subject to Modification and Extension (April or May 2020)*. Puisque le développement de l'Application est sujet à changement, il y a des risques que des mises à jour ne priorisant pas la sécurité et la confidentialité soient introduites. Quant au **Framework API**, ils donnent des instructions pour créer une application de suivis des contacts (*contact tracking*).¹³

Nous connaissons les oppositions face à une telle application et les dérives possibles des gouvernements. Ces applications peuvent aussi être utilisées pour surveiller le confinement. La Chine a imposé en février 2020 une application pour contrôler les déplacements de leur population.

¹⁰ COVID-19, surveillance and the threat to your rights. Amnesty International 04/03/20

¹¹ *A Scramble for Virus Apps That Do No Harm*. New York Time 06/03/20
<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

¹² *A Scramble for Virus Apps That Do No Harm*. New York Time 06/03/20
<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

¹³<https://www.apple.com/covid19/contacttracing>

« In February, China began requiring residents in more than 200 cities to download a health code app that automatically dictates whether people must quarantine. »¹⁴

En Inde, les applications servent d'ailleurs principalement à contrôler la quarantaine et non à détecter les contacts entre des personnes atteintes de Covid-19 et des personnes saines. En effet, une application utilisée dans l'état indien de Maharashtra, où se trouve Mumbai, fonctionne en recueillant la géolocalisation et les données GPS des utilisateurs pour créer un périmètre virtuel qui doit être respecté, sans quoi les autorités sont alertées. L'application de suivi de contacts utilisée dans l'état indien de Karnataka recueille également la localisation des utilisateurs et leur demande de prendre des égo-portraits afin de prouver qu'ils sont bel et bien à la maison. Le gouvernement fédéral a introduit une application utilisant le GPS et le Bluetooth afin de recueillir de l'information sur les déplacements des utilisateurs et sur les autres appareils avec lesquels ils ont été en contacts. ¹⁵

Les technologies utilisées par les applications de suivi de contacts par différents pays et états varient. Certaines applications utilisent la technologie de géolocalisation et la technologie sans-fil *Wi-Fi* plutôt que le *Bluetooth*. D'autres utilisent une combinaison des différentes technologies disponibles.

Par exemple, dans l'État du *North Dakota*, l'application de suivi de contacts utilisée fonctionne avec le *Wi-Fi*, les tours de téléphonie cellulaire et la position GPS afin de localiser les individus. Cette approche est moins précise pour détecter les contacts entre individus et elle est plus intrusive quant à la surveillance. L'application permet seulement aux individus atteints de la Covid-19 de dire au personnel de suivi de contacts où ils se trouvaient avant d'avoir leur diagnostic. ¹⁶

À Singapour, l'application utilisée fonctionne par la technologie Bluetooth en détectant les téléphones cellulaires à proximité du téléphone de l'utilisateur. Les données personnelles et les

¹⁴ *A Scramble for Virus Apps That Do No Harm. New York Time 06/03/20*

<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

¹⁵ *A Scramble for Virus Apps That Do No Harm. New York Time 06/03/20*

<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

¹⁶ *A Scramble for Virus Apps That Do No Harm. New York Time 06/03/20*

<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

informations sont conservées directement sur l'appareil de l'utilisateur sauf si ce dernier accepte de partager certaines informations avec le personnel de suivi de contacts, après avoir reçu un résultat positif, pour qu'il puisse en informer d'autres individus qui auraient pu être exposé au virus SARS-CoV-2.¹⁷

Parmi toutes ces applications, la mise en garde provient aussi des informaticiens qui présentent également cette dualité entre contenir la pandémie et les droits de la protection à la vie privée et les renseignements personnels. Effectivement, plusieurs experts indiquent que le meilleur moyen d'empêcher le gouvernement d'utiliser les données privées des citoyens pour les surveiller est de s'assurer que le gouvernement n'ait jamais accès à ces données. Lors d'événements majeurs les conséquences sur le droit à la vie privée sont souvent ignorées afin d'assurer la sécurité ou la santé du public.¹⁸

Nous reconnaissons que de recueillir les données de localisation pourrait faciliter le suivi de contacts. En effet, Lalitesh Katragadda, le fondateur d'Indihood avance que: "Having location history helps you better identify where infections might be, helps you identify the hot spots,".¹⁹ Nous croyons cependant que les risques de conserver les données personnelles d'utilisateurs dans un serveur central pose un risque bien plus grand que les possible bénéfices.

Par conséquent, la ligne apparaît mince entre les objectifs de contenir une pandémie et de contrôler la ou des populations. En effet, un gouvernement à l'obligation de garantir le droit à la santé en contrôlant et prévenant les épidémies. Ce même gouvernement peut donc temporairement restreindre certains droits de façon proportionnelle, comme celui à la vie privée, afin de répondre à la situation de crise. Il est primordial que les mesures prises par les gouvernements soient

¹⁷ *A Scramble for Virus Apps That Do No Harm. New York Time 06/03/20*
<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

¹⁸ *A Scramble for Virus Apps That Do No Harm. New York Time 06/03/20*
<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

¹⁹ *A Scramble for Virus Apps That Do No Harm. New York Time 06/03/20*
<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

proportionnelles et temporaires tout en suivant des critères stricts sans quoi elles pourraient être considérées illégales et l'outil développé pourrait être banni comme en Norvège. ^{20, 21}

Amnistie Internationale soulève le fait que certaines applications de suivi de contacts et de localisation utilisent l'intelligence artificielle ce qui augmente le danger que des individus ou communautés marginalisés soient confrontés à plus de discriminations. En effet, ces technologies utilisent des algorithmes opaques, c'est-à-dire qu'il nous est impossible d'évaluer l'analyse effectuée par ceux-ci. De plus, les critères utilisés par ces algorithmes sont souvent basés sur des données biaisées. ^{22, 23, 24} Les communautés marginalisées sont souvent plus vulnérable face à la pandémie actuelle, il est donc primordial de s'assurer de ne pas exacerber leur marginalisation et les désavantages auxquels ils sont confrontés.

Certaines compagnies privées ont aussi développé des outils de surveillance. Il faut donc y surveiller les abus et protéger le droit à la vie privée des individus. Les collaborations publique-privée peuvent présenter une piste de solution dans plusieurs domaines et évidemment en santé, mais cela peut s'avérer inquiétant si l'on regarde l'historique des compagnies privées qui propose ces solutions. C'est effectivement le cas aux États-Unis où certaines compagnies telles que Clearview AI et Palantir sont en pourparlers avec le gouvernement. Amnistie Internationale rapporte également que la compagnie Israélienne NSO Group, vend un outil d'analyse de données personnelles qui permettrait de suivre la propagation du virus en analysant les déplacements des citoyens. Cette compagnie a un historique plutôt négatif quant à l'abus des droits de la personne. C'est pourquoi il est primordial de s'assurer de la réputation des compagnies privées qui proposent ce type d'outils avant d'envisager une collaboration. ²⁵

²⁰ COVID-19, surveillance and the threat to your rights. Amnesty International 04/03/20

²¹ *Virus-Tracing Apps Are Rife with Problems. Governments Are Rushing to Fix Them. The New York Time* 07/08/20

²² McKay, J. (n.d.). AI-Based Location Positioning System for Private Contact Tracing. Retrieved from <https://www.govtech.com/em/safety/-AI-Based-Location-Positioning-System-for-Private-Contact-Tracing.html>

²³ COVID-19, surveillance and the threat to your rights. Amnesty International 04/03/20

²⁴ Council of Europe. (2019, February 11). Discrimination, Artificial Intelligence and Algorithmic Decision-Making. Retrieved from <https://www.coe.int/en/web/artificial-intelligence/-/news-of-the-european-commission-against-racism-and-intolerance-ecri->

²⁵ COVID-19, surveillance and the threat to your rights. Amnesty International 04/03/20

Il faut également éviter de se précipiter dans une solution trop rapide. L'exemple du Qatar est probant:

« An investigation by Amnesty's [Security Lab](#) discovered the critical weakness in the configuration of Qatar's EHTERAZ contact tracing app. Now fixed, the vulnerability would have allowed cyber attackers to access highly sensitive personal information, including the name, national ID, health status and location data of more than one million users. »²⁶

En développant l'application de suivi de contacts trop rapidement, le gouvernement du Qatar laissait une vulnérabilité majeure pouvant être exploitée par les cybercriminels. De plus, le gouvernement du Qatar avait rendu l'utilisation de l'application obligatoire ce qui exposait la population entière à un risque de fraude élevé. La vulnérabilité, bien que corrigée rapidement par le gouvernement, n'aurait jamais dû exister. ²⁷

Il importe de souligner que le *modus operandi* des cybercriminels ne correspond pas à celui des « criminels traditionnels ». Ces derniers cherchent généralement une cible potentielle avant de définir leur plan, les cybercriminels, dans bien des cas, identifient des vulnérabilités pour, par la suite, commettre un délit. Les cybercriminels collaborent généralement à distance avec un réseau selon leurs spécialités et leurs capacités à utiliser les failles. Ils ne cherchent pas l'opportunité, ils la créent.

Comme démontré dans les dernières années les nouvelles technologies comportent souvent d'importantes vulnérabilités. Par contre, les vulnérabilités Bluetooth sont rarement discutées. Bien qu'il soit vrai que l'utilisation du Bluetooth soit moins intrusive que la technologie de géolocalisation (GPS) et ne collecte pas directement de données personnelles, elle comporte des vulnérabilités permettant à certains cybercriminels d'avoir accès à ces données. Il appert que le Bluetooth soit réputé pour n'être détectable que sur de courtes distances et qu'il soit difficile d'en

²⁶ Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million. Amnesty International 05/26/20

²⁷ Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million. Amnesty International 05/26/20

extraire des informations, cependant il n'est pas impossible pour des pirates informatiques d'utiliser le « reverse engineering » pour obtenir accès aux données d'un tiers en utilisant les failles de sécurité. Certains outils ont été développés afin d'obtenir accès aux échanges entre les appareils utilisant Bluetooth tel qu'un téléphone et une paire d'écouteur permettant ainsi à une tierce personne d'écouter une conversation téléphonique. En effet, il est possible d'étendre le « range » de détection d'un appareil Bluetooth en utilisant d'autres appareils ou des balises Bluetooth.²⁸

Des vulnérabilités Bluetooth connues portent le nom de BlueBorne. Cette collection de failles permettait à des pirates informatiques d'installer des « malwares » et d'effectuer des attaques sur les autres appareils en utilisant le Bluetooth. « Bluetooth mesh networking » rend cette vulnérabilité encore plus grave puisque les pirates pourraient sauter d'un appareil à l'autre facilement. Avec BlueBorne, l'attaquant commence par détecter un appareil Bluetooth à proximité avant d'identifier son adresse MAC unique. Cette dernière lui permet d'identifier le système d'exploitation de l'appareil et d'ajuster son attaque avant de la déployer.²⁹

Une autre vulnérabilité connue est BleedingBits, des puces électroniques installées dans plusieurs types d'appareils. Celles-ci permettaient des attaques sans même que l'attaquant ne soit jumelé avec l'appareil en question ou qu'il ait des connaissances antérieures de cet appareil.³⁰

Certaines vulnérabilités permettent d'obtenir la clef d'encryptions utilisé par un appareil et de l'utiliser afin d'obtenir des données et de falsifier certaines informations. Des chercheurs en sécurité de l'université de Boston ont découvert qu'ils pouvaient identifier les appareils utilisés lors d'une connexion par technologie Bluetooth malgré que les identifiants étaient cryptés par l'appareil. De plus, lorsque le niveau de sécurité Bluetooth n'est pas maximal, certaines informations sont échangées sans encryptions entre les différents appareils, ce qui accroît les risques puisque l'information n'a pas à être « hackée », mais elle peut plutôt être déduite à partir de l'information interceptée par un tiers.³¹

²⁸ <https://www.sentinelone.com/blog/bluetooth-attacks-dont-let-your-endpoints-down/>

²⁹ <https://www.sentinelone.com/blog/bluetooth-attacks-dont-let-your-endpoints-down/>

³⁰ <https://www.sentinelone.com/blog/bluetooth-attacks-dont-let-your-endpoints-down/>

³¹ <https://www.dailymail.co.uk/sciencetech/article-7258715/amp/Security-researchers-uncover-Bluetooth-vulnerability-let-hackers-track-LOCATION.html>

La sécurité standard de la technologie Bluetooth inclue deux étapes d'authentifications, soit : *legacy authentication procedure* et *secure authentication procedure*. Celles-ci utilisent une clef d'encryptions. Ces mesures sont supposées empêcher les attaques par usurpation aussi appelées BIAS (Bluetooth Impersonation AttackS). Une équipe de chercheurs européen provenant d'Oxford et de l'école polytechnique fédérale de Lausanne a démontré que même la technologie la plus récente de Bluetooth était vulnérable à ce type d'attaques. Cette équipe a attaqué différents types d'appareils possédants des puces électroniques des systèmes d'exploitation différents les uns des autres afin de montrer que ceux-ci ne sont pas à l'abris des attaques par Bluetooth.³²

Bien que BlueBorne et BleedingBits soient les vulnérabilités les plus connues et qu'elles aient été corrigées, elles ne sont pas les seules qui ont été détectées. Effectivement, en février dernier BlueFrag, une nouvelle vulnérabilité critique a été détectée. Celle-ci a également été corrigée peu de temps après sa détection, mais elle démontre que de nouvelles mises à jour des systèmes d'exploitation des appareils électroniques peuvent toujours introduire de nouvelles vulnérabilités. En effet, Niels Schweissheim, directeur du programme HackerOne, estime que le Bluetooth et ses futures utilisations ne seront jamais à l'abris de nouvelles failles.^{33, 34}

Pour le chercheur Jan Ruge de la Technische Universität Darmstadt, le meilleur moyen de se protéger contre des attaques utilisant le Bluetooth est de désactiver celui-ci lorsqu'il n'est pas en utilisation. Par contre, comme l'application AlerteCovid utilise le Bluetooth, il serait nécessaire de laisser le Bluetooth de l'appareil activé en tout temps, ce qui accroît les risques d'exploitation d'une faille. Dans cette perspective, il faut être d'autant plus vigilant avec les appareils mobiles fournis par l'employeur afin de ne pas mettre à risque le système de l'employeur. D'un autre point de vue, l'aspect de l'autorisation de l'employeur pour utiliser ce type d'outils peut avoir un impact sur la réussite de son déploiement. À ce même titre, qu'en est-il des outils utilisés par certains

³² Antonioli, D., Tippenhauer, N. O., & Rasmussen, K. (2020). BIAS: Bluetooth Impersonation AttackS. 2020 *IEEE Symposium on Security and Privacy (SP)*. doi:10.1109/sp40000.2020.00093

³³ <https://www.sentinelone.com/blog/bluetooth-attacks-dont-let-your-endpoints-down/>

³⁴ <https://www.zdnet.fr/actualites/contact-tracing-attention-aux-vulnerabilites-du-bluetooth-39902823.htm>

employeurs pour contrôler l'utilisation de leur matériel? De plus, est-ce que ceux-ci pourraient être tentés d'accéder aux informations personnelles pour d'autres fins.³⁵

Il est important de noter que nous n'avons pas présentement pas accès à tous les détails concernant les protocoles de sécurité et le niveau d'encryptions utilisés présentement par les outils proposés.

De plus, Stas Protassov, co-fondateur et président de la technologie d'Acronis, émet une mise en garde puisqu'il croit que certaines applications malveillantes imitant l'application officielle pourraient être mises en circulation. Il est donc primordial que seule l'application officielle soit téléchargée afin d'assurer la confidentialité des données personnelles des utilisateurs.³⁶

Un autre exemple de dérive est l'application utilisée en Norvège, suspendue temporairement par le gouvernement en juin. Ensuite, l'organisme de surveillance du pays a imposé une interdiction provisoire de l'application *Smittestopp* en juillet. Finalement l'application a été bannie puisqu'elle présentait plus de risques que de bénéfices étant donné le nombre de cas de Covid-19 répertorié en Norvège. Cette application, lancée en avril, enregistrait les utilisateurs qui avait été à proximité d'autrui pendant plus de 15 minutes, en analysant les données GPS et *Bluetooth* des appareils, et les alertaient s'ils avaient été exposé au coronavirus SARS-CoV-2. Les informations recueillies par l'application étaient conservées sur un serveur central et pouvaient être consultées par les autorités gouvernementale. Près d'un cinquième des norvégiens de plus de 16 ans utilisaient l'application avant sa suspension.^{37, 38}

Ces exemples concrets démontrent l'importance de ne pas prioriser la rapidité du lancement de l'application plutôt que la sécurité liée à cet outil technologique. Comme précédemment mentionné, il est primordial que la population ait confiance en son gouvernement et en

³⁵ <https://www.tomsguide.com/news/android-bluetooth-hack>

³⁶ <https://www.zdnet.fr/actualites/contact-tracing-attention-aux-vulnerabilites-du-bluetooth-39902823.htm>

³⁷ *Virus-Tracing Apps Are Rife with Problems. Governments Are Rushing to Fix Them. The New York Times* 07/08/20

³⁸ *A Scramble for Virus Apps That Do No Harm. New York Times* 06/03/20

<https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>

l'application de suivi de contacts si l'application doit jouer un rôle dans le contrôle de la pandémie de Covid-19.

Amnistie Internationale, rapporte qu'environ 45 pays planifie utiliser un type d'application de suivi de contacts malgré les risques de sécurité majeures que ce type d'outils technologiques pose.³⁹

Pour les gouvernements qui vont actualiser une application de suivis des contacts, l'Organisation Mondiale de la Santé (OMS) a établi un guide dans son texte « Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance ».⁴⁰ Dans ce texte, l'OMS traite des différents aspects liés à l'utilisation des applications de suivi de contacts. L'utilisation de telles applications doit être temporaire et proportionnelle à la menace de la pandémie actuelle. De plus, il est important que ces applications soient testées par des agences et comités indépendants pour s'assurer de leur bon fonctionnement et de l'absence de failles de sécurité. Seulement l'information nécessaire au suivi de contacts doit être recueilli par l'application et cette information ne devrait en aucun cas être vendues pour des usages commerciaux ou autres que ceux directement liés à la santé publique. L'information des utilisateurs devrait être conservée de façon à assurer un maximum de confidentialité et de sécurité et ce uniquement pour la durée nécessaire pour faire face à la pandémie. L'utilisation d'applications de suivi de contacts devrait être volontaire et le tout devrait se faire de façon transparente pour que les utilisateurs puissent faire un choix éclairé. Il est primordial qu'il n'y ait pas d'abus de ce type de technologie par des gouvernements ou compagnies privées.⁴¹

Les aspects et recommandations présentées par l'OMS doivent être étudiés et suivis de façon responsable si un gouvernement souhaite utiliser une application de suivi de contacts de façon optimale et sécuritaire.

³⁹ Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million. Amnesty International 05/26/20

⁴⁰ Voir Annexe I

⁴¹ Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Interim Guidance. World Health Organization. 05/28/20

Le gouvernement canadien a prévu faire des essais en Ontario en juillet avec une application nommée *Covid Alert* qui doit être installée de manière volontaire par les individus. L'utilisateur doit télécharger sur un téléphone intelligent cette application qui permet de voir si l'utilisateur a été en contact avec un individu infecté par le virus SARS-CoV-2. Selon un reportage sur Global news, cette application n'amasserait pas les données personnelles et protégerait la vie privée. Elle ne collecterait pas la localisation GPS et détecterait les contacts par la proximité entre deux appareils intelligents via la technologie sans-fil Bluetooth en échangeant des codes aléatoires toutes les cinq minutes avec les téléphones à proximité. Cette application serait développée par Apple et Google et serait en attente de l'autorisation du commissaire à la vie privée. Les données recueillies par l'application s'effaceraient après 14 jours.^{42, 43} De plus, en Allemagne, ce même type d'applications serait déjà à l'essai.⁴⁴

Le fait que l'application canadienne *Covid Alert* ne fonctionne que sur les appareils intelligents de marque Apple ou Android de fabrication récente avec mise à jour récente du système d'exploitation soulève une importante préoccupation. En effet, les communautés les plus à risque et qui bénéficieraient le plus de l'utilisation d'une telle application, se trouveront donc à être ceux qui n'y ont pas accès. En effet, il est reconnu que « les Noirs, les Autochtones, les personnes de couleur »⁴⁵, les personnes sans-domicile fixe et les personnes plus démunies sont les personnes généralement plus à risque et les plus touchées par la pandémie.⁴⁶ CBC rapportait le 30 juillet dernier que les Noirs et les personnes de couleur représentaient 83% des cas de COVID-19 à Toronto alors qu'ils ne représentent qu'environ la moitié de la population.⁴⁷ Global news rapporte également qu'historiquement les pandémies affectent plus les communautés autochtones. Ces communautés sont souvent défavorisées, n'ayant pas accès aux mêmes ressources que nos

⁴² <https://globalnews.ca/news/7080914/coronavirus-ontario-covid-19-tracing-app/>

⁴³ <https://www.droit-inc.com/article27155-6-questions-a-Me-Gratton-sur-l-application-Alerte-COVID>

⁴⁴ <https://www.lesoleil.com/actualite/monde/lallemagne-mise-sur-les-portables-et-le-bluetooth-contre-lepidemie-781bb94c289d731e46f2926bca39552b>

⁴⁵ Christopher Parsons, associé de recherche principal au Citizen Lab, Munk School of Global Affairs and Policy, Université de Toronto

⁴⁶ <https://www.lapresse.ca/covid-19/2020-08-03/les-problemes-d-accessibilite-de-l-application-alerte-covid-critiques.php>

⁴⁷ <https://www.cbc.ca/news/canada/toronto/toronto-covid-19-data-1.5669091>

communautés.⁴⁸ Ces communautés sont aussi celles qui ont plus difficilement accès aux outils technologiques proposés. ⁴⁹

L'Alberta propose à sa population sa propre application : ABTraceTogether. Sur son site web le gouvernement albertain définit son application de la manière suivante :

« ABTraceTogether is a mobile contact tracing app that helps to let you know if you've been exposed to COVID-19 – or if you've exposed others – while protecting your privacy (with an anonymous ID). »⁵⁰

Pourtant la commissaire à l'information et à la vie privée de l'Alberta (OIPC) Jill Clayton a déclaré:

«[Clayton noted] safeguards are out of Alberta Health's control, but said nonetheless, there is still a security risk because, to run the app, Apple devices need to remain unlocked, "which significantly increases risk in case of theft or loss.»⁵¹

Il y a des risques à créer et instaurer une application pour le suivi des contacts. En plus des risques d'intrusions et de vols de données, d'autres risques sont introduits avec les restrictions du fonctionnement de l'application utilisée comme démontré par l'application ABTraceTogether.⁵²

Le choix d'une application ne doit pas avoir de ratés, car le succès de cet outil dépendra de la confiance de la population. La mise en œuvre d'une application de suivi de contacts doit faire l'objet d'examens rigoureux afin de déterminer si les risques sont proportionnels aux bénéfices

⁴⁸ <https://globalnews.ca/news/7201390/coronavirus-covid-19-indigenous-people-support-second-wave/>

⁴⁹ <https://www.lapresse.ca/covid-19/2020-08-03/les-problemes-d-accessibilite-de-l-application-alerte-covid-critiques.php>

⁵⁰ <https://www.alberta.ca/ab-trace-together.aspx>

⁵¹ <https://globalnews.ca/news/7159859/alberta-covid-19-coronavirus-tracking-app-risks/>

⁵² <https://globalnews.ca/news/7159859/alberta-covid-19-coronavirus-tracking-app-risks/>

apportés par son utilisation. Il est essentiel de mesurer l'efficacité et les impacts que ce genre de technologie peut avoir à court terme et à long terme. ⁵³

En conclusion, le succès d'une application de notification des contacts ou de suivis de contacts dépend en grande partie de la confiance du public envers la fiabilité de l'outil et du gouvernement ou de l'organisme qui le met en œuvre. Il est primordial de ne pas sacrifier le droit à la vie privée et la sécurité pour un outil technologique dont les bienfaits ne sont pas garantis. Si toute fois une application est utilisée, afin de protéger les données personnelles, celles-ci doivent être analysées localement dans le téléphone de l'utilisateur et aucune donnée ne doit être collectée et stockée dans un serveur centralisé par le gouvernement. Si une application plus intrusive était utilisée et que les données des usagers étaient stockées dans un serveur localisé, les réseaux criminels pourraient y obtenir accès comme démontré par les nombreuses fuites de données au cours des dernières années. De plus, puisque l'application proposée par le gouvernement canadien n'est pas accessible à tous, cela diminue grandement son efficacité. Instaurer une telle application est basée sur l'hypothèse qu'elle sera efficace pour contenir d'éventuelles éclosions, selon une analyse de risque, les écoles seraient un site de transmission important. Si tel est le cas, la mesure discutée aujourd'hui n'aurait que peu ou pas d'impact sur cette nouvelle éclosion. C'est pourquoi l'instauration d'une application de notification de contacts présente plus de risques que de bienfaits.

⁵³ Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Interim Guidance. World Health Organization. 05/28/20

BIBLIOGRAPHIE

1. World Health Organization, (2015, July 23). *Contact tracing*, Retrieved from <https://www.who.int/csr/disease/ebola/training/contact-tracing/en/>
2. Swaan, Corien M.; Appels, Rolf; Kretzschmar, Mirjam E. E.; van Steenbergen, Jim E. (2011-12-28). "Timeliness of contact tracing among flight passengers for influenza A/H1N1 2009". *BMC Infectious Diseases*. **11** (1): 355. doi:10.1186/1471-2334-11-355.
3. Global Health Ethics Unit (2020, May 28). Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. *World Health Organization*, Retrieved from https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1
4. Jeffords, A. J. (2020, June 19). Coronavirus: Ontario piloting new COVID-19 contact tracing app, launch expected July 2. Retrieved from <https://globalnews.ca/news/7080914/coronavirus-ontario-covid-19-tracing-app/>
5. Laurin-Desjardins, C. (2020, August 5). 6 questions à Me Gratton sur l'application Alerte COVID. Retrieved from <https://www.droit-inc.com/article27155-6-questions-a-Me-Gratton-sur-l-application-Alerte-COVID>
6. Apple, Google, (2020, May) <https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf>
7. Wells, N. (2020, August 03). Les problèmes d'accessibilité de l'application Alerte COVID critiqués. Retrieved from <https://www.lapresse.ca/covid-19/2020-08-03/les-problemes-d-accessibilite-de-l-application-alerte-covid-critiques.php>
8. Johnson, B. (2020, May 11). Nearly 40% of Icelanders are using a covid app-and it hasn't helped much. Retrieved from <https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/>
9. Valentino-devries, J., Singer, N., & Krolik, A. (2020, April 29). A Scramble for Virus Apps That Do No Harm. Retrieved from <https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>
10. Amnesty International, (2020, April 03). COVID-19, surveillance and the threat to your rights. Retrieved from <https://www.amnesty.ca/blog/covid-19-surveillance-and-threat-your-rights>

11. Apple and Google. (n.d.). Privacy-Preserving Contact Tracing. Retrieved from <https://www.apple.com/covid19/contacttracing/>
12. Singer, N. (2020, July 08). Virus-Tracing Apps Are Rife With Problems. Governments Are Rushing to Fix Them. Retrieved from <https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html>
13. McKay, J. (n.d.). AI-Based Location Positioning System for Private Contact Tracing. Retrieved from <https://www.govtech.com/em/safety/-AI-Based-Location-Positioning-System-for-Private-Contact-Tracing.html>
14. Council of Europe. (2019, February 11). Discrimination, Artificial Intelligence and Algorithmic Decision-Making. Retrieved from <https://www.coe.int/en/web/artificial-intelligence/-/news-of-the-european-commission-against-racism-and-intolerance-ecri>
15. Amnesty International (2020, May 26). Contact tracing app exposed sensitive personal details of over one million. Retrieved from <https://www.amnestyusa.org/press-releases/contact-tracing-app-security-flaw-exposed-sensitive-personal-details-of-more-than-one-million/>
16. SentinelOne (2019, June 10). Bluetooth Attacks | Don't Let Your Endpoints Down Retrieved from <https://www.sentinelone.com/blog/bluetooth-attacks-dont-let-your-endpoints-down/>
17. Pero, J. (2019, July 17). Security researchers uncover Bluetooth vulnerability that could let hackers track your LOCATION. Retrieved from <https://www.dailymail.co.uk/sciencetech/article-7258715/amp/Security-researchers-uncover-Bluetooth-vulnerability-let-hackers-track-LOCATION.html>
18. Antonioli, D., Tippenhauer, N. O., & Rasmussen, K. (2020). BIAS: Bluetooth Impersonation AttackS. 2020 IEEE Symposium on Security and Privacy (SP). doi:10.1109/sp40000.2020.00093
19. Yu E. (2020, April 27). Contact tracing : Attention aux vulnérabilités du bluetooth. Retrieved from <https://www.zdnet.fr/actualites/contact-tracing-attention-aux-vulnerabilites-du-bluetooth-39902823.htm>
20. Wagenseil, P. (2020, February 07). Most Android phones can be hacked via Bluetooth right now: What to do. Retrieved from <https://www.tomsguide.com/news/android-bluetooth-hack>
21. Foulkes, M. (2020, April 05). *Agence France-Presse*, L'Allemagne mise sur les portables et le bluetooth contre l'épidémie. Retrieved from <https://www.lesoleil.com/actualite/monde/lallemagne-mise-sur-les-portables-et-le-bluetooth-contre-lepidemie-781bb94c289d731e46f2926bca39552b>

22. Cheung, J. (2020, July 30). Black people and other people of colour make up 83% of reported COVID-19 cases in Toronto. Retrieved from <https://www.cbc.ca/news/canada/toronto/toronto-covid-19-data-1.5669091>
23. Bowden, O. (2020, July 21). Indigenous people need more support to weather 2nd wave of COVID-19: experts. Retrieved from <https://globalnews.ca/news/7201390/coronavirus-covid-19-indigenous-people-support-second-wave/>
24. ABTraceTogether. (n.d.). Retrieved from <https://www.alberta.ca/ab-trace-together.aspx>
25. Slugoski, K. (2020, July 10). Alberta's COVID-19 contact-tracing app a 'security risk' on Apple devices: Privacy commissioner. Retrieved from <https://globalnews.ca/news/7159859/alberta-covid-19-coronavirus-tracking-app-risks/>

Annexe I – Ethical considerations to guide the use of digital proximity
tracking technologies for COVID-19 contact tracing: Interim guidance
World Health Organization

Principle	Explanatory Text
Time limitation	All measures shall be temporary in nature and limited in scope. If governments and health systems expand monitoring and surveillance powers then such powers should be time bound, and only continue for as long as necessary to address the current pandemic. Measures should be fully withdrawn at the earliest moment after the epidemic has ended locally. There are legitimate concerns that digital proximity tracking will be unnecessary yet will remain in place.
Testing and evaluation	Digital proximity tracking technologies are novel and largely untested in many countries and settings. Every effort should be made to test the technologies prior to widespread use to ensure they function as intended, are technically robust, and have no security flaws. Governments and health systems should implement rigorous evaluation of the technology during the pandemic to continuously monitor that it is working effectively. The evaluations should be conducted by an independent agency or research body and should be published.
Proportionality	Collection and processing of personal data and health data shall be proportionate and provided by law. This means that collection of data for digital proximity tracking must be (a) justified by legitimate public health objectives; (b) suitable to achieve the intended goal; (c) necessary; and (d) reasonable and proportionate to the aims pursued. The latter requirement entails assessing the value of colliding rights vis-à-vis the impact intensity of surveillance activities on each person. The least intrusive (privacy-preserving) measures should always be preferred for an application's design, including avoiding the use of physical location (geographic position) tracking for digital proximity tracking.
Data minimization	Data collection, retention and processing shall be limited to the minimum necessary amount

	of data that is needed to achieve the public health objective. Thus, data collection should not require the identity or location data of a user, or a time stamp of a proximity event (though the date of a proximity event may be useful). Data collected, retained and aggregated must be limited in scope.
Use restriction	The sale and use of data for commercial purposes or advertising activities should be strictly prohibited. Recognizing that governments may have existing data protection laws and frameworks already in place, the sharing of data with government departments, agencies or third parties that are not involved in the public health response should be prohibited. The sharing of data with law enforcement or immigration departments or agencies should also be prohibited.
Voluntariness	An individual's decision to download and use an application that contributes to public health surveillance or digital proximity tracking should be voluntary and informed. Governments should not mandate use of such an application. Additional incentives or inducements by either a government or private parties should not be offered to individuals who download and use such an application. No individual should be denied services or benefits from either a government or private parties for refusing to use an application, including the right to use health services, the receipt of economic aid in the context of a pandemic or thereafter, or the use of a phone that is provided by a company for work-related purposes. An individual should be free to turn off the application at any time and should be free to delete the application at any time, without any consequences, as well as to delete any data that may have been collected and stored, including retroactively redacting blocks of time that the user does not wish to upload.
Transparency and explainability	Data collection and processing shall be transparent, and individuals shall be provided

	with concise and reader-friendly information in clear and unambiguous language regarding the purpose of collection, the types of data collected, how data will be stored and shared, and how long data shall be retained. There should be full transparency about how the applications and application programming interfaces (APIs) operate, and publication of open source and open access codes. Individuals should also be provided with meaningful information about the existence of automated decision-making and how risk predictions are made, including how the algorithmic model was developed and the data used to train the model. Furthermore, there should be information about the model's utility and insights as to the types of errors that such a model may make.
Privacy-preserving data storage	There are differing views as to whether data storage should be decentralized or centralized, including which approach to data storage is more effective and secure. Both approaches may preserve privacy but both approaches also have vulnerabilities that must be addressed, including the security of data that are collected and stored. There is an emerging consensus, including opinions issued recently by several data protection authorities, that decentralized approaches enhance privacy, since they provide users with greater control (including the exercise of consent or withdrawal of consent) over the quantum of information that a user may share with health authorities. The collection and use of such data by health authorities can therefore be limited to what is strictly necessary for the operation of a digital proximity tracking system. Whichever approach is selected, governments and third parties should ensure it is in conformity with expectations of privacy and the principles included in this guidance.
Security	Every effort should be made to ensure high security, including encryption, of any personal data or health data collected and of any devices, applications, servers, networks, or services involved in collection, transmission, processing, and storage. Applications should be subject to third-party audits and penetration testing, and

	developers should publish full details about their security protocols.
Limited retention	Data retention shall be limited to the period of the pandemic response, except for the purposes of research or epidemic planning, subject to appropriate regulation, oversight and informed consent, where required. Data used for research purposes or epidemic planning should be aggregated and anonymized where possible. Where aggregation of data is not possible for research purposes, such exceptions should be justified, and all such data should still be anonymized. Data collected for public health purposes related to COVID-19 shall be deleted following the pandemic. To the extent technically feasible, any technological system created should be dismantled at the end of the pandemic.
Infection reporting	The reporting into a digital proximity tracking application that a user has tested positive for COVID-19 could be done through several channels. In any scenario, notification of the application should require the consent of the individual. In one scenario, a user of a digital proximity tracking application could self-report an infection to the application. A health system must determine if such self-notification must be confirmed by a health professional. Alternatively, upon a patient being confirmed as positive for COVID-19, a medical professional could notify the digital proximity tracking application (with the individual's consent).
Notification	Notification of individuals who may have been in contact with a person infected with COVID-19 could, for example, be delivered directly by an application to close contacts. The notification of other users must preserve the privacy of the infected individual. Users who receive a notification through their device should receive information on the steps they should take. Such notification should be provided in clear, accessible language and explain the options that users have (including any consequences attached to these options). Such notification should be accessible to all people. This information should be provided in several languages and be accessible to people with disabilities. Users should be able to consent as to whether they wish to have the health authorities contact them for follow-up (for example, testing), including disclosure of their contact information to

	the health authorities. A user who has been notified by an application should not be penalized, punished or denied medical services or economic benefits for failing to follow instructions provided by the application.
Tracking of COVID-19-positive cases	After an individual who uses a digital proximity tracking application has tested positive for COVID-19, the application should not be used to track that individual's movements during his or her period of infection and recovery, including whom that individual may encounter thereafter.
Accuracy	Algorithmic models used to process data and assess risk of transmission must be reliable, verified and validated. Such applications should be open to testing by third parties and risk models should be developed with epidemiologists to establish parameters for duration and proximity before a contact is recorded and should be adjusted and improved over time. Data quality should be assessed for biases to avoid any adverse effects, including giving rise to unlawful and arbitrary discrimination.
Accountability	Any response must incorporate accountability protections and safeguards against abuse. Individuals must be given the opportunity to know about and challenge any COVID-19-related measures to collect, aggregate, retain and use data. Individuals subjected to unwarranted surveillance must have access to effective remedies and mechanisms of contestation.