May 22, 2020

Statement on privacy-respecting and trust-worthy COVID-19 tracing apps

(version francaise si-dessous - for the French version see below)

In an effort to track the spread of COVID-19, more and more COVID-19 tracing apps have and will continue to emerge. Canadian jurisdictions are developing and deploying contact-tracing apps without sufficient technical review by independent security and privacy experts. We, the undersigned, believe this practice should change. Such reviews help identify potential flaws and provide indispensable input to a public debate about the balance between health safety, privacy and security. Reviews can enhance trust in the deployment of apps and help foster wider adoption. Reviews should be public because public technical specifications will enhance trust and acceptance.

The Canadian security and privacy ecosystem, including the academic community, consists of sufficiently many experts to provide such reviews. Such reviews should be made with the mandate of protecting civil liberties and held to the highest ethical and technical standards. We have compiled an evolving list of guidelines on the development, design and deployment of these apps that can enhance privacy and cybersecurity. These guidelines can be used as a reference in a review, albeit the need for interpretation in the context of a particular app.

To ensure core principles of Canada's western liberal democracy are protected, a set of best practices should be established to guarantee that a tracing app is developed and deployed in a safe way. We address contact tracing apps, which is software deployed on a mobile device (e.g. cell phone or wearables) specifically designed to detect contacts with other such devices to indicate its owner has been sufficiently close to facilitate the potential transmission of a COVID-19 infection. It may be tempting to use tracing information collected by these apps for other reasons beyond contact tracing. These secondary purposes should be weighed against privacy concerns because this will increase public acceptance and use of the tracing app.

Tracing apps will be inherently privacy-risky. Their core functionality is to identify those who may have come in contact with COVID-19 or individuals who have the disease. Thus, the highest possible standard must be applied to its design, development, and deployment.

To ensure public health safety and to guarantee protection of Canadians' rights, we believe the following principles should be applied to the development and deployment of any tracing app:

Independent expert review: The design and implementation of the app should be subject to open independent expert review by software security and privacy experts in advance of deployment. Such a review ensures that the objectives of privacy protection have been properly implemented.

Simple design: The app should be developed using the simplest approach possible to facilitate a timely and verifiable review of the implementation to ensure it conforms to the reviewed design specification and pertinent principles of data protection. This includes a review of the source code on both the app and any supporting servers.

Minimal functionality: The app should only provide the necessary functionality to allow for contact tracing and there should be no additional code incorporated into the app. There should be no secondary

purpose embedded in the app. Any additional functionality must be part of the review. A consequence of secondary functionality will be a longer public debate about the value of deploying the app.

Data minimization: The only data collected should be what is required for contact tracing purposes. Whenever possible, contacts (and any other required app data) should be retained on the device where they are collected and should only be shared with other users or to a central repository if required for a contact tracing incident. Any data collected and stored creates an obligation to properly manage this data, complicating the design of the app.

Trusted data governance: If data is transmitted to a central repository, the repository must be a trustworthy actor subject to public oversight. A government or health sector agency subject to investigation by privacy commissioners/ombudspersons should be used to store contact data and no private sector data repositories should be allowed access to contact data. A properly managed central repository can enforce data protection and cybersecurity of sensitive data.

Cybersecurity: A tracing app is part of Canada's critical infrastructure with the potential to send many people into isolation or quarantine. Hence, the highest level of cybersecurity must be implemented for all aspects of the contact tracing app, including the collection of the data on the device, the tracing app itself, the communication channels used to move data, and any central locations. All malicious attacks should be considered. This includes audits and monitoring to ensure breaches do not occur or are contained if they do.

Minimum data retention: The data collected should only be retained for the lifetime of its intended purpose. For COVID-19, data should only be retained for the infectious period for the person carrying the device and any data stored centrally (or with other devices) should be permanently deleted after it has been used for the contact tracing required.

Protection of derived data and meta-data: Derived data and meta-data allows for sensitive inferences about the app's users. Derived data should only be used with consent and should be protected by mechanisms to prevent re-identification. No meta-data should be collected, stored, or used in the analysis of contact traces.

Proper disclosure and consent: The user must be made aware, in a clear and understandable way, what data is collected about them and how it is used. If there are uses for this data beyond the contact tracing functionality, these must be made explicit and separate consent received for each such use. This disclosure and consent should be renewed regularly to ensure both the ongoing need for the tracing functionality and the users' commitment to continuing to participate.

Provision to sunset: There should be provisions to sunset the app and delete its collected data after the COVID-19 crisis is contained. Data collection should be automatically terminated and notification of all participants should occur. Any residual data should be deleted as soon as the app is no longer used.

For press inquiries you may contact Florian Kerschbaum <florian.kerschbaum@uwaterloo.ca> or Ken Barker <kbarker@ucalgary.ca>

Déclaration sur les applications de traçage COVID-19 respectueuses de la vie privée et dignes de confiance

Afin de suivre la propagation de COVID-19, de plus en plus d'applications de traçage COVID-19 ont vu le jour et continueront de le faire. Les juridictions canadiennes développent et déploient des applications de traçage des contacts entre personnes sans que des experts indépendants en matière de sécurité et de protection de la vie privée ne procèdent à un examen technique suffisant. Nous, les soussignés, pensons que cette pratique devrait changer. De tels examens permettent d'identifier les failles potentielles et apportent une contribution indispensable à un débat public sur l'équilibre entre la santé, la protection de la vie privée et la sécurité. Ces examens peuvent renforcer la confiance dans le déploiement des applications et contribuer à en favoriser une plus large adoption. Les évaluations devraient être publiques car des spécifications techniques publiques renforceront la confiance et l'acceptation.

L'écosystème canadien de la sécurité et de la protection de la vie privée, y compris la communauté universitaire, est composé d'un nombre suffisant d'experts pour fournir de telles évaluations. Ces évaluations doivent être réalisées dans le but de protéger les libertés civiles et être conformes aux normes éthiques et techniques les plus élevées. Nous avons dressé une liste évolutive de lignes directrices sur le développement, la conception et le déploiement de ces applications qui peuvent améliorer la protection de la vie privée et la cybersécurité. Ces lignes directrices peuvent être utilisées comme référence dans le cadre d'un examen, même s'il est nécessaire de les interpréter dans le contexte d'une application particulière.

Afin de garantir la protection des principes fondamentaux de la démocratie libérale occidentale du Canada, un ensemble de meilleures pratiques devrait être établi pour garantir qu'une application de traçage est développée et déployée de manière sécuritaire. Nous nous intéressons aux applications de traçage de contact entre personnes, c'est-à-dire aux logiciels déployés sur un appareil mobile (par exemple un téléphone portable ou autre dispositif portable) spécialement conçus pour détecter les contacts avec d'autres appareils de ce type afin d'indiquer que son propriétaire a été suffisamment proche pour faciliter la transmission potentielle d'une infection COVID-19. Il peut être tentant d'utiliser les informations de traçage cueillies par ces applications pour d'autres raisons que le traçage de contacts entre personnes. Ces objectifs secondaires doivent être contrastés avec les préoccupations relatives à la protection de la vie privée, car cela permettra d'accroître l'acceptation et l'utilisation de l'application de traçage par le public.

Les applications de traçage seront intrinsèquement risquées pour la vie privée. Leur fonction principale est d'identifier les personnes qui ont pu être en contact avec le COVID-19 ou les personnes atteintes de la maladie. Il faut donc appliquer la norme la plus élevée possible à sa conception, son développement et son déploiement.

Pour assurer la santé publique et garantir la protection des droits des Canadiens, nous pensons que les principes suivants doivent être appliqués au développement et au déploiement de toute application de traçage:

Examen par des experts indépendants: La conception et la mise en œuvre de l'application devraient faire l'objet d'un examen ouvert par des experts indépendants en sécurité logicielle et en protection de

la vie privée avant le déploiement. Un tel examen permet de s'assurer que les objectifs de protection de la vie privée ont été correctement mis en œuvre.

Conception simple: L'application doit être développée en utilisant l'approche la plus simple possible pour faciliter un examen opportun et vérifiable de la mise en œuvre afin de s'assurer qu'elle est conforme à la spécification de conception révisée et aux principes pertinents de protection des données. Cela comprend l'examen du code source autant de l'application que celui sur les serveurs qui la supportent.

Fonctionnalité minimale: L'application ne doit fournir que les fonctionnalités nécessaires pour permettre le traçage des personnes et aucun code supplémentaire ne doit être intégré à l'application. Aucune fonction secondaire ne doit être intégrée à l'application. Toute fonctionnalité supplémentaire doit faire partie de l'examen. Une des conséquences de l'ajout d'une fonctionnalité supplémentaire sera un débat public plus long sur l'intérêt de déployer l'application.

Minimisation des données: Les seules données collectées doivent être celles qui sont nécessaires au traçage des contacts. Dans la mesure du possible, les contacts (et toute autre donnée requise par l'application) doivent être conservés sur l'appareil où ils sont collectés et ne doivent être partagés avec d'autres utilisateurs ou vers un dépôt central que si cela est nécessaire pour un incident de contact entre personnes. Toute donnée cueillie et stockée crée une obligation de gérer correctement ces données, ce qui complique la conception de l'application.

La Gouvernance des données de confiance: Si les données sont transmises à un dépôt central, celui-ci doit être un acteur digne de confiance et soumis au contrôle public. Un organisme gouvernemental ou du secteur de la santé faisant l'objet d'une enquête par les commissaires à la protection de la vie privée/ombudsmans doit être utilisé pour stocker les données de contact et aucun dépôt de données du secteur privé ne doit être autorisé à accéder aux données de contact. Un dépôt central correctement géré peut faire respecter la protection des données et la cybersécurité des données sensibles.

Cybersécurité: Une application de traçage fait partie de l'infrastructure critique du Canada et peut envoyer de nombreuses personnes en isolement ou en quarantaine. Par conséquent, le plus haut niveau de cybersécurité doit être mis en œuvre pour tous les aspects de l'application de traçage des personnes, y compris la cueillette des données sur le dispositif, l'application de traçage elle-même, les canaux de communication utilisés pour transférer les données et tout emplacement central. Toutes les attaques malveillantes doivent être prises en compte. Cela comprend les audits et la surveillance afin de s'assurer que des incidents de pénétration ne se produisent pas ou qu'elles sont maîtrisées si elles se produisent.

Conservation minimale des données: Les données cueillies ne doivent être conservées que pendant la durée de vie de leur utilisation prévue. Pour le COVID-19, les données ne doivent être conservées que pendant la période infectieuse pour la personne portant le dispositif et toute donnée stockée de manière centralisée (ou avec d'autres dispositifs) doit être supprimée de manière permanente après avoir été utilisée pour le traçage des contacts nécessaire.

Protection des données et métadonnées dérivées: Les données et métadonnées dérivées permettent de faire des déductions sensibles sur les utilisateurs de l'application. Les données dérivées ne doivent être utilisées qu'avec le consentement de l'utilisateur et doivent être protégées par des mécanismes

empêchant leur réidentification. Aucune métadonnée ne doit être cueillie, stockée ou utilisée dans l'analyse des traçages de contact entre personnes.

Divulgation et consentement appropriés: L'utilisateur doit être informé, de manière claire et compréhensible, des données cueillies à son sujet et de la manière dont elles sont utilisées. Si ces données sont utilisées à d'autres fins que la fonction de traçage des personnes, il est obligatoire d'obtenir un consentement explicite et distinct pour chacune de ces utilisations. Cette divulgation et ce consentement doivent être renouvelés régulièrement afin de garantir à la fois le besoin récurrent de fonctionnalité de traçage et l'engagement des utilisateurs à continuer à participer.

Disposition d'extinction: Il devrait y avoir des dispositions pour mettre fin à l'utilisation de l'application et supprimer les données cueillies après que la crise du COVID-19 ait été maîtrisée. La cueillette de données devrait être automatiquement interrompue et tous les participants devraient en être informés. Toute donnée résiduelle devrait être supprimée dès que l'application n'est plus utilisée

Relations de presse: contactez Florian Kerschbaum <florian.kerschbaum@uwaterloo.ca> ou Ken Barker <kbarker@ucalgary.ca>

Carleton University

David Barrera; Robert Biddle; Jason Jaskolka; Lianying Zhao

Concordia University

Otmane Ait Mohamed; Chadi Assi; Jeremy Clark; Mourad Debbabi; Martin French; Mohsen Ghafouri; Kash Khorasani; Walter Lucia; Mohammad Mannan; Fenwick McKelvey; Arash Mohammadi; Jun Yan; Amr Youssef

McGill University

Benjamin C. M. Fung

Memorial University

Jonathan Anderson

Ontario Tech University

Rajen Akalu; David Clark; Khalil El-Khatib; Shahram S. Heydari; Patrick Hung; Andrea Slane; Julie Thorpe

Polytechnique Montréal

Nora Boulahia-Cuppens; Frédéric Cuppens; José M. Fernandez; Gabriela Nicolescu

Queen's University

Jianbing Ni; Mohammad Zulkernine

Royal Military College of Canada

Sylvain P. Leblanc

Ryerson University

Atefeh Mashatan; Ali Miri

University of Alberta

Karim Ali

University of British Columbia

Karthik Pattabiraman; Konstantin Beznosov

University of Calgary

Ken Barker; Philip Fong; Allen Habib; Gregory Hagen; Ryan Henry; Thomas P. Keenan; Emily Laidlaw; Raymond Patterson; Joel Reardon; Rei Safavi-Naini; Barry Sanders; Renate Scheidler; Svetlana Yanushkevich

University of Guelph

Ali Dehghantanha; Xiaodong Lin; Deborah Stacey

University of Manitoba

Noman Mohammed

Université de Montréal

Benoit Dupont

University of New Brunswick

Scott Bateman; Ali Ghorbani; Arash Habibi Lashkari; Rongxing Lu; Kalikinkar Mandal; Brent Petersen; Suprio Ray

University of Ottawa

Carlisle Adams; Anne Broadbent; Céline Castets-Renard; Amy Felty; Guy-Vincent Jourdan; Vivek Krishnamurthy; Jason Millar; Teresa Scassa