

# Consultations particulières et 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

MEMOIRES

CAPT(RET) STEVE WATERHOUSE, CD



13 août 2020



## Introduction

C'est un honneur et un privilège de m'adresser à vous sur un sujet l'heure.

Tout d'abord, voici une brève introduction de mes origines. Après 23 ans de service avec les Forces armées canadiennes et au Ministère de la Défense Nationale (MDN), j'ai eu le privilège d'être parmi les premiers « cyber-soldats » au pays, passant par la gestion des systèmes d'information en réseau de la taille d'un réseau local (LAN - 250 utilisateurs), d'un réseau de campus (CAN - 650 utilisateurs) à celle d'un réseau métropolitain (MAN - plus de 5000 utilisateurs sur plusieurs sites), jusqu'aux premières phases d'intégration de la cybersécurité à titre d'Officier de Sécurité des Systèmes d'Information (OSSI) pendant 10 ans, principalement à la renaissance du Collège militaire royal de Saint-Jean (CMRSJ). Plus récemment, outre les divers mandats de consultation avec mon entreprise INFOSECSW, je continue cette mission d'éduquer et former tant les novices que les professionnels des technologies de l'information (TI) et à sensibiliser le public sur la manière d'appliquer les meilleures pratiques de sécurité envers les TI, principalement avec l'Université de Sherbrooke<sup>1</sup> et aussi via les médias d'information (locaux et nationaux) et par la présentation de conférences au pays et ailleurs dans le monde.

## La situation

L'année 2020 a débuté sans que nous nous doutions qu'elle marquerait l'évolution de notre société. De tous les scénarios que j'ai déjà étudiés pour préparer les systèmes d'information que j'avais sous ma responsabilité, celui du bactériologique a toujours été sous-considéré. Et tel que constaté ces derniers mois, il y a des pratiques de base qui doit être maintenue, telles que la gestion sécuritaire de l'information, peu importe le contexte.

À partir de Tel Aviv (Israël) en fin janvier 2020 j'étais avec une délégation internationale de journalistes et de professionnels en sécurité de l'information, et peu se souciait comment se développait la situation en Chine, qui dégénérait chaque jour. Il était facile à comprendre qu'à moins de fermer TOUTES les frontières (terrestres, aériennes et maritimes), tous les pays seraient affectés en peu temps (ce qui est arrivé). À mon retour au pays, devant le « build-up » de la situation en février, peut aussi se préoccupait de cette continuité des opérations en cas d'isolement total (scénario extrême) et surtout, comment continuer le travail. Dans un contexte nucléaire, radiologique ou chimique, les détecteurs et conséquences sont un plus facile à discerner, mais là en plein hiver, durant la saison de la grippe et du rhume pour nous, le bactériologique est moins évident à percevoir. Alors, comment anticiper et documenter ce nouveau risque et surtout, comment continuer à travailler ?

Au début mars, alors que les cas en Europe se multiplient rapidement, les pays avec une gouvernance plus ferme se sont tournés vers leurs services policiers et/ou de renseignement pour voir comment suivre les infectés de ceux considérés non-infectés (difficile sans tests, car peu ou pas de signes apparents). Les outils de traçabilité de première instance considérés à ce moment sont évidemment le thermomètre frontal

à l'arrivée à l'aéroport<sup>2 3</sup> (mesure utilisée lors des cas de contamination passée du SRAS et autres), suivi GPS des téléphones cellulaires<sup>4</sup>, puis les caméras thermiques<sup>5</sup> (faisant même apparition dans nos épiceries). Or, l'efficacité de ces moyens est limitée. Les thermomètres ont été prouvés et classés comme inefficaces à détecter les asymptomatiques tout comme les caméras thermiques. Cependant, les autorités de santé publique devant aucun moyen de détection ont choisi l'isolement et les mesures de quarantaine. Dès le début, la question essentielle était sur toutes les lèvres : Comment s'assurer que les gens en quarantaine ou qu'un citoyen déclaré COVID-19 positif demeure(nt) isolé(s) tout en respectant la confidentialité des renseignements personnels et la vie privée ?

## Qu'est-ce qui devrait être fait ?

La Commission d'éthique des sciences et des technologies (CEST) a publié un rapport<sup>6</sup> à la fin avril élaborant bien les considérations fondamentales en matière de protection de la vie privée et de la protection des renseignements personnels. Ce sont là de très bonnes bases pour le développement éventuel d'applications de recherche numérique de contacts (appelé aussi application de notification d'exposition).

En partant de cette réflexion, les programmeurs ont des lignes directrices raisonnables pour démarrer la conception. Cependant, la technologie étant ce qu'elle est, il y a là matière à bien comprendre les enjeux quant aux limites de cette technologie. Sans dériver trop dans le *catastrophisme*<sup>7</sup>, il y a ces quelques préoccupations quant aux limites des applications de recherche numérique de contacts, énumérées par le *Canadian Medical Association Journal (CMAJ)*.<sup>8</sup>

1. L'efficacité de ces applications dépend de leur adoption par la population : le potentiel d'une telle application correspond au carré de la fraction de ses utilisateurs dans une population;
2. Les technologies qui sous-tendent les applications comportent des erreurs de mesure qui limitent leur efficacité à identifier les contacts;
3. Les approches basées sur la technologie Bluetooth qui n'utilisent pas le système Apple–Google seront limitées par les restrictions de balayage Bluetooth pour les téléphones intelligents fonctionnant avec iOS;
4. De manière générale, par rapport à la recherche manuelle de contacts, la surveillance constante et à grande échelle au moyen d'applications de recherche des contacts soulève plus de problèmes en ce qui concerne la protection des renseignements personnels
5. Même si des études de modélisation ont laissé entendre que les applications de recherche des contacts permettraient de réduire la transmission, aucune étude n'a été publiée en ce sens

Or, la Linux Fondation<sup>9</sup> a colligé la majorité des méthodes de conception des applications et de documentation des données ainsi que les pays qui les utilisent afin de lancer leur application de traçage COVID (Annexe « A »). Certains pays sont pour le suivi pur et dur via GPS (comme au Bahreïn, au Koweït, en Norvège<sup>10</sup> ou en Corée du Sud<sup>11</sup>) alors que les modèles plus orientés vers la protection de la vie privée sont développés avec le cadre de travail GAEN<sup>12</sup>. Malgré les différentes méthodes employées, seulement 9.3 % de la population parmi les 13 pays les plus peuplés de la planète ont adopté une application soit de suivi ou de notification d'exposition<sup>13</sup>. Certains scientifiques ont avancé qu'il doit y avoir un taux d'adoption entre 60-70% dans la population pour avoir des résultats efficaces<sup>14</sup>. Alors que certains autres mentionnent que seulement 15% est nécessaire. Les faits sont quand même éloquentes alors que seulement 5 pays de 22 sondés ont franchi la barre du 15% d'adoption<sup>15</sup>.

L'application canadienne « COVID Alerte » mise en disponibilité le 31 juillet 2020<sup>16</sup> est un produit développé à partir du cadre GAEN et du code « COVID Shield »<sup>17</sup>, contrairement à l'application de suivi de l'Alberta « ABTraceTogether » (déployée le 1<sup>er</sup> mai) qui elle est basée sur le modèle déployé au Singapour appelé « TraceTogether »<sup>18</sup> utilisant le protocole « BlueTrace »<sup>19</sup> (Taux d'acceptation de 5.3% après 3 mois d'opération comparé à moins de 4% pour COVID Alerte après 6 jours)<sup>20</sup>. Le choix que l'Ontario et du Gouvernement du Canada ont fait d'utiliser la technologie GAEN et COVID Shield semble rencontrer ce désire des citoyens et des commissaires à la protection de la vie privée et des renseignements personnels à réduire au minimum les risques de fuites d'information personnelle et d'identification des utilisateurs.<sup>21</sup>

## Qu'est-ce qui peut mal aller ?

La fiabilité du signal Bluetooth est à retenir comme étant peu exemplaire en termes de précision considérant l'emplacement de l'appareil et par la nature de la transmission omnidirectionnelle. Il y a quelques mois, le collège de Trinité de Dublin a produit deux évaluations qui démontrent comment le signal se propage et la précision des résultats dans des environnements variables<sup>22 23</sup>.

Outre l'imprécision qu'offre la technologie Bluetooth, fondamentalement les appareils opérants à partir du système d'exploitation Android ont été démontrés avec des façons de faire innées dans ce système d'exploitation, laissant couler de l'information qui permet d'identifier l'utilisateur plus facilement<sup>24</sup>. Ces failles reconnues par Google ne seront corrigées qu'à la prochaine version d'Android soit vers la fin du mois de septembre 2020<sup>25</sup>. Il s'agit d'un facteur quand même important à considérer, car cela représente près de la moitié des utilisateurs au pays dont les informations permettant de les identifier, seront plus facilement accessibles que les usagers des appareils Apple iOS.

Il y a aussi la considération de nuisance malicieuse (évalué à peu probable) qui pourrait s'en prendre à la technologie Bluetooth par l'induction d'interférence (four à micro-ondes, Wi-Fi, autres appareils utilisant Bluetooth car la fréquence 2.4 GHz sur laquelle opère le Bluetooth sera toujours susceptible d'interférence compte tenu de la grande activité sur cette bande de fréquences) ou par des attaques de personnification (BIAS)<sup>26</sup> envers son protocole (évalué à peu probable), tout comme l'exploitation de la vulnérabilité du protocole Bluetooth BLE (gATTack)<sup>27</sup> elle aussi évaluée à peu probable de se matérialiser.

Les plus vieux types d'attaques tels que BlueBug, BlueSnarfing, BlueJacking ou BlueSmack sont à toutes fins impraticables depuis la version 4.0 de Bluetooth présent sur les appareils modernes<sup>28</sup>. Le risque est donc très faible de voir des attaques de ces types réussir.

## Recommandations

Le Québec a 3 choix :

- A. Développer pour le MSSS une application / s'arrimer avec un modèle d'application déjà en production tout en demeurant indépendant. Ce choix implique l'isolation des données en provenance de l'extérieur, puisque les citoyens qui visitent autres lieux au pays auront à utiliser d'autre application;
- B. Joindre l'initiative fédérale afin d'assurer la continuité dans l'échange des données, et;
- C. Ne pas investir dans le développement et l'administration d'applications de notification d'exposition et continuer le suivi manuel comme c'est actuellement;

La Norvège en juin dernier a suspendu l'usage de son application sur les bases de faible taux d'infection et du risque élevé de compromission de la vie privée des citoyens<sup>29</sup>. Tout comme le Royaume-Unis, l'Allemagne et l'Australie qui vivent des difficultés techniques avec les applications qui remettent en question les résultats perçus<sup>30 31</sup>. Alors considérant l'absence de moyens fiables pour détecter le dit virus « COVID-19 » préalablement mentionné, considérant le besoin de connaître les tendances immédiates et anticiper ce qui est à venir, considérant les 5 facteurs énoncés du CMAJ et surtout en considérant les failles technologiques présentes et à venir pour miner la vie privée et les renseignements personnels du citoyen, je suis d'avis d'opter pour l'option « C ».

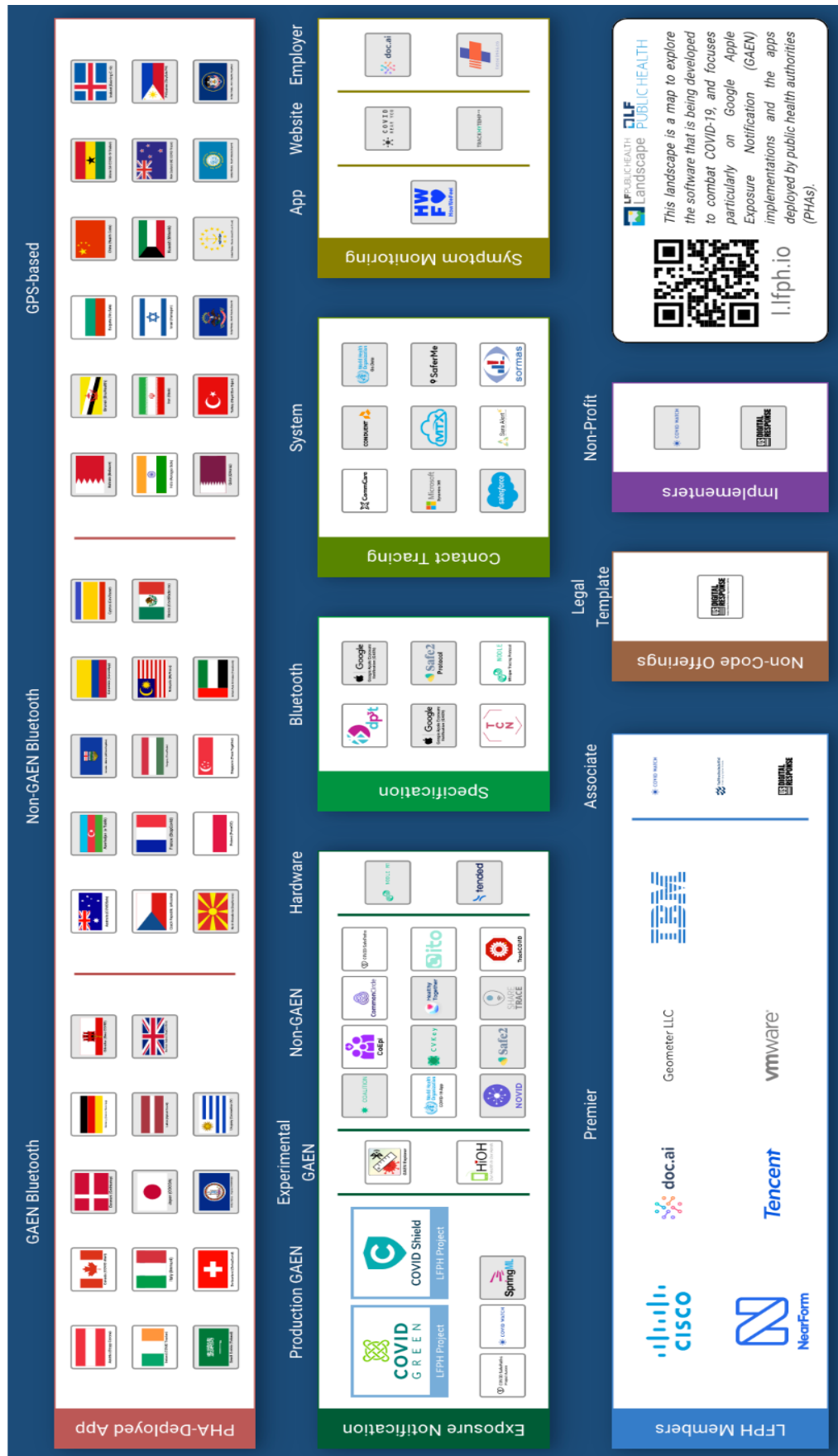
Dans l'éventualité que le choix d'utiliser une application de notification d'exposition soit considéré et décidé, je recommande que l'option « B » soit retenue afin de rapidement effectuer le déploiement et assurer au québécois et aux autres citoyens du pays l'échange d'information nécessaire afin que tous soient avisés de leur niveau de risque d'infection.

En conclusion, ma crainte la plus grande dans la mise en circulation de ces applications demeure la diminution de la vigilance des gens qui ne voudront se fier que sur l'avertissement de contamination possible de leur téléphone portable au lieu de continuer d'appliquer les mesures d'hygiène de base telles que le port du masque, le lavage des mains et la distanciation physique. L'application ne sera alors que source de distraction davantage que source d'information utile.

Je suis maintenant disponible à répondre à vos questions.

Merci

Annexe A  
Tableau des différentes applications COVID-19



Linux Fondation Public Health Landscape – 07 août 2020  
<https://landscape.lfph.io/>

## Annexe B

### Références

- <sup>1</sup> CeFTI - Centre de formation en technologies de l'information - Microprogramme de 2e cycle en sécurité informatique - volet prévention (À distance) (<https://www.usherbrooke.ca/cefti/futurs-etudiants/microprogramme-de-2e-cycle-en-securite-informatique-volet-prevention-a-distance/>)
- <sup>2</sup> Effectiveness of airport screening at detecting travelers infected with novel coronavirus (2019-nCoV) ([https://www.eurosurveillance.org/content/10.2807/1560-7917.ES.2020.25.5.2000080#html\\_fulltext](https://www.eurosurveillance.org/content/10.2807/1560-7917.ES.2020.25.5.2000080#html_fulltext))
- <sup>3</sup> No US coronavirus cases were caught by airport temperature checks. Here's what has worked (<https://www.cnn.com/2020/02/19/health/coronavirus-airport-temperature-checks/index.html>)
- <sup>4</sup> Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? (<https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price>)
- <sup>5</sup> Infrared Temperature Devices for Infectious Disease Screening During Outbreaks: Overview of an ECRI Evidence Assessment (<https://cadth.ca/sites/default/files/covid-19/ha0004-non-contact-ir-temperature-screening-final.pdf>)
- <sup>6</sup> Rapport d'étape sur les conditions d'acceptabilité éthique - 22 avril 2020 – ([https://www.ethique.gouv.qc.ca/media/1329/cest-conditions-acceptabilite-ethique\\_v7.pdf](https://www.ethique.gouv.qc.ca/media/1329/cest-conditions-acceptabilite-ethique_v7.pdf))
- <sup>7</sup> LaPresse+ – 19 mai 2020 - Entre le technosolutionnisme et le catastrophisme ([http://mi.lapresse.ca/screens/a6b42637-0450-4ae8-bddd-a890d5809da7\\_7C\\_0.html](http://mi.lapresse.ca/screens/a6b42637-0450-4ae8-bddd-a890d5809da7_7C_0.html))
- <sup>8</sup> Recherche numérique des contacts dans le contexte de la COVID-19 (<https://www.cmaj.ca/content/cmaj/suppl/2020/06/11/cmaj.200922.DC1/200922-ana-fr.pdf>)
- <sup>9</sup> LF Public Health Landscape (<https://landscape.lfph.io/category=exposure-notification&grouping=category&zoom=150>)
- <sup>10</sup> Les applications de traçage des contacts de Bahreïn, du Koweït et de la Norvège figurent parmi les plus dangereuses pour le droit au respect de la vie privée (<https://www.amnesty.org/fr/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/>)
- <sup>11</sup> MOBILITY CRISIS AND RESPONSE IN THE TIME OF COVID-19: THE REPUBLIC OF KOREA'S APPROACH ([https://www.iom.int/sites/default/files/documents/mobility\\_crisis\\_and\\_response\\_in\\_the\\_time\\_of\\_covid19\\_rok\\_approach\\_final\\_0518.pdf](https://www.iom.int/sites/default/files/documents/mobility_crisis_and_response_in_the_time_of_covid19_rok_approach_final_0518.pdf))
- <sup>12</sup> Apple-Google Privacy-Preserving Contact Tracing (<https://www.apple.com/covid19/contacttracing>)
- <sup>13</sup> COVID-19 Contact Tracing Apps Reach 9% Adoption In Most Populous Countries COVID-19 Contact Tracing App Screenshot (<https://sensortower.com/blog/contact-tracing-app-adoption>)
- <sup>14</sup> A mathematically rigorous assessment of the efficiency of quarantining and contact tracing incurring the COVID-19 epidemic (<https://www.medrxiv.org/content/10.1101/2020.05.04.20091009v1.full.pdf>)
- <sup>15</sup> Global contact tracing app downloads lag behind effective levels (<https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels/>)
- <sup>16</sup> Une nouvelle application mobile pour aider à informer les Canadiens d'une exposition possible à la COVID-19 est maintenant disponible (<https://pm.gc.ca/fr/nouvelles/communiqués/2020/07/31/nouvelle-application-mobile-aider-informer-les-canadiens-dune>)
- <sup>17</sup> COVID Shield Exposure notification solution (<https://www.covidshield.app/>)
- <sup>18</sup> TraceTogether (<https://www.tracetogogether.gov.sg/>)
- <sup>19</sup> BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders ([https://bluetrace.io/static/bluetrace\\_whitepaper-938063656596c104632def383eb33b3c.pdf](https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf))
- <sup>20</sup> Less than 4% of Canadians have the COVID Alert tracing app — despite better privacy protection than Facebook (<https://www.thestar.com/business/2020/08/05/just-13-million-canadians-have-downloaded-covid-alert-will-that-be-enough-to-be-effective.html>)
- <sup>21</sup> Appuyer la santé publique et bâtir la confiance des Canadiens : principes de protection de la vie privée et des renseignements personnels pour les applications de traçage des contacts et autres applications similaires ([https://priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2020/s-d\\_20200507/](https://priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2020/s-d_20200507/))
- <sup>22</sup> Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection ([https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth\\_rssi\\_study.pdf](https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf))
- <sup>23</sup> Measurement-Based Evaluation of Google/Apple Exposure Notification API For Proximity Detection In A Commuter Bus (<https://arxiv.org/pdf/2006.08543.pdf>)
- <sup>24</sup> Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps ([https://www.scss.tcd.ie/Doug.Leith/pubs/contact\\_tracing\\_app\\_traffic.pdf](https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf))
- <sup>25</sup> Google Company Announcements - An update on Exposure Notifications (<https://blog.google/inside-google/company-announcements/update-exposure-notifications>)
- <sup>26</sup> 20200518 - BIAS: Bluetooth Impersonation AttackS paper (<https://francozappa.github.io/about-bias/publication/antonioli-20-bias/antonioli-20-bias.pdf>)
- <sup>27</sup> GATTACKING BLUETOOTH SMART DEVICES (<https://raw.githubusercontent.com/securing/docs/master/whitepaper.pdf>)
- <sup>28</sup> Potential Bluetooth Vulnerabilities in Smartphones (<https://pdfs.semanticscholar.org/bdf3/f7d786aee3fa29059d782bc41736bdf68c20.pdf>)
- <sup>29</sup> Norway: Halt to COVID-19 contact tracing app a major win for privacy (<https://www.amnesty.org/en/latest/news/2020/06/norway-covid19-contact-tracing-app-privacy-win/>)
- <sup>30</sup> Coronavirus: The great contact-tracing apps mystery (<https://www.bbc.com/news/technology-53485569>)
- <sup>31</sup> Germany's coronavirus tracing app criticized over warning failures (<https://www.dw.com/en/germanys-coronavirus-tracing-app-criticized-over-warning-failures/a-54305099>)