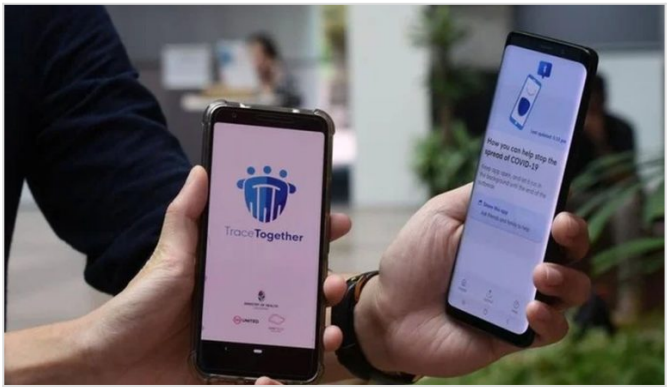
Tracer le virus, contrôler les populations. Il s'appelle Robert, il aime le gruyère



L'application StopCovid est en marche. Pardon, en phase de développement. Et le gouvernement se veut le plus transparent possible pour provoquer l'adhésion de la population, en affichant l'objectif de respect de la vie privée, du contrôle utilisateur, de l'ouverture du code source, voire même du nom des développeurs. L'application n'est pas prête, mais les spécifications du protocole établis par l'INRIA sont publiées. Le protocole porte le nom de Robert (ROBust and privacy-presERving proximity Tracing). Voilà, Robert doit maintenant séduire. Mais Robert, c'est juste Robert, pas Redford.

Plus il y a de gruyère, plus il y a de trous

Avant de parler composition et recette de l'application, reprenons déjà les conditions objectives ainsi que les seuils minimaux d'usage :

- Pour avoir une utilité, donc un impact, l'application doit être téléchargée et installée sur 75 % des équipements mobiles du territoire.
- Or les terminaux mobiles n'étant pas aptes à recevoir une telle application représentent déjà 25 % du parc existant (fracture numérique matérielle).
- Une partie des appareils compatibles est utilisée par des personnes dont les compétences manquent pour installer et activer correctement l'application (fracture numérique d'usage, qui impacte surtout les personnes âgées, également les plus vulnérables au Covid-19).
- L'asynchronie des expériences épidémiques et des mesures similaires a fait choux blanc ; comme à Singapour, dans des conditions matérielles autrement plus favorables. Ces échecs ne peuvent que ralentir et freiner l'adoption d'une telle solution chez le public équipé et compétent.

Non seulement les conditions objectives ne sont pas mûres en France, mais en plus la stratégie de l'avant-garde, identique à celle des pays mûrs, s'est déjà cassée la gueule méchamment.

Mais plus il y a de trous, moins il y a de gruyère

Parlons recettes, compositions, affinage, mais tout d'abord ustensiles :

- L'application passe par l'usage du bluetooth et nécessite donc son activité constante.

L'impact sur la batterie est faible, mais le bluetooth connaît lui aussi des failles de sécurités, dont une, particulièrement grave, a été découverte en 2017. Si la faille a certainement été corrigée sur tous les modèles sortis après la découverte, quid des modèles précédents ? En temps normal, l'usage ponctuel du bluetooth suffit pour « solution de contournement » mais, avec StopCovid, on parle d'un usage constant, donc d'une exposition constante d'une vulnérabilité à qui saura l'exploiter. A la date du 22 avril, plusieurs médias évoquent des demandes des gouvernements auprès des constructeurs de smartphones comme Apple, Samsung et beaucoup d'autres, qui bloquent par défaut l'usage du bluetooth par des applications tournant en arrière plan (ce que sera l'application StopCovid). Mesure standard de sécurité.
- À défaut d'être tracé.e.s par l'État, vous le serez par des entités privées et capitalistes, notamment dans les centres commerciaux où de nombreuses bornes tracent les appareils par bluetooth et wifi, et par recoupement d'informations, construisent des profils, identifient, et émettent des offres ciblées.

Pour l'aspect tambouille et ingrédients, Robert fonctionne avec un serveur central générant des « pseudonymes » uniques pour chaque application. Une déclaration d'infection (*a priori* contrôlée par le corps médical) d'un ou d'une utilisatrice ne renvoie au serveur central que les pseudonymes collectés précédemment (et pas son propre pseudonyme), c'est-à-dire les pseudonymes des personnes avec un potentiel contact avec celle déclarée infectée. Lors de sa connexion quotidienne, l'application d'un tiers vérifie si elle fait partie des pseudonymes ayant été mis sur la liste des mis en contact avec un.e infecté.e.

Pour les risques, le parallèle est assez similaire : du côté de l'État on reste *clean* dans la manière de traiter les données. [1] Ce sont là encore des détournements individuels ou organisationnels qui peuvent impliquer des desseins malveillants[2]. De multiples scénarios sont possibles, et nous renvoyons à l'élaboration https://risques-tracage.fr pour quelque chose de plus exhaustif. Nous indiquons simplement quelques détournements possibles :

- **Espionnage assez simple :** utilisez un téléphone à usage unique avec l'application et allumez le uniquement devant la personne que vous soupçonnez malade. Si vous recevez une notification, alors cette personne est bien infectée. L'anonymisation des données vole en éclat. Aucune compétence informatique n'est requise… :
- **Espionnage par recoupement d'informations :** vous voulez savoir qui vous a contaminé. Dans vos de contacts, demandez si ils et elles ont reçu l'alerte, et petit à petit éliminez les possibilités pour arriver à l'individu.e « coupable ». Là encore, aucune compétence informatique n'est requise…
- **Fausse alerte volontaire :** il est très facile, là encore sans compétence informatique, d'imaginer des stratagèmes pour déclencher des fausses alertes volontairement (attacher son téléphone sur son chien qui court dans un parc toute la journée, emprunter le téléphone d'une personne contaminée pour générer un lot d'alerte dans son lieu de travail/d'étude, etc.).
- **L'espionnage collectif :** à l'image des repérages de radars via les applications de

circulation routière, on peut aisément imaginer la naissance d'application tierces, qui récoltent et croisent les données StopCovid fournies par les utilisateurs pour déterminer les malades.
- **L'espionnage par des cybercriminel.le.s** qui par des applications pirates (une application qui cache un virus par exemple) récupèrent les informations sur la maladie, et s'en servent pour faire du chantage.
- **Du fichage à grande échelle par des grandes entreprises** qui n'hésitent pas à collecter des informations personnelles illégalement dans le but de les monnayer (des exemples récents existent, comme le scandale Cambridge Analytica, et nous permettent de penser cela) .

En résumé nous avons donc une application qui, par la fragmentation logicielle et l'absence de continuité de maintenance et mise à jour, permet de possibles malveillances « classiques », mais qui, en plus, ouvre de nouvelles possibilités de captation, d'exploitation, et de croisement de données – notamment de santé ! – à des entités tierces. **En prétendant contribuer à la sécurité sanitaire, StopCovid participe à la vulnérabilité des appareils et des données (de santé) personnelles.**

Donc plus il y a de gruyère, moins il y a de gruyère

Robert n'est ni utile, ni sexy, ni subtil. On pourrait en rire d'avance pour le couac, mais ça n'en ferait pas non plus un humoriste. Non seulement la fracture numérique, tant en terme d'accès aux équipements qu'à leur maîtrise, ne permet même pas d'atteindre les seuils nécessaires à rendre l'application utile dans cette période de pandémie, mais en plus elle expose toutes celles et ceux qui feraient bonne volonté de l'installer à des actes de malveillances, de croisements, d'exploitations de données, d'identification, par des techniques et moyens nombreux étrangers à l'application StopCovid, mais qui prennent appui sur son utilisation ou sur l'usage des technologies (bluetooth) nécessaires à son fonctionnement.

L'application StopCovid ne saurait être un outil utile pour la maîtrise actuelle de l'épidémie, ni en confinement, ni en déconfinement. Au regard de ce que cette application permet – et surtout ne permettra pas – et des dangers que son usage comporte nous appelons toutes celles et ceux qui liraient cet article à ne pas installer cette application. A convaincre autour d'elles et d'eux. Et à combattre, au futur, toute tentative d'imposition d'un système de tracking.

Notes

1. À la date du 22 avril, des débats techniques et d'ingénieries ont lieu publiquement sur le github de développement de l'application StopCovid ; il existe des échanges sur la manière d'assurer la sécurité de l'implémentation du protocole.

2. Et nous renvoyons à cette fantastique élaboration qui détaille de façon précise et

pédagogique ce qui sera brièvement exposé ici : https://risques-tracage.fr/docs/risque--tracage.pdf

Frédérick Lorie, le 24 avril 2020