Risques et limites des applications de traçage covid-19

Véronique Cortier, CNRS - Loria
(Nancy, France)
https://members.loria.fr/VCortier/

Co-auteur d'un *document grand public sur les risques des applications de traçage* avec un groupe de 14 chercheurs

transparents préparés avec l'aide de Gaëtan Leurent

Note : toutes les parties en italiques sont « cliquables » et pointent vers des références.

Les promesses de StopCovid

- *Sa conception permet que PERSONNE, pas même l'Etat, n'ait accès à la liste des personnes diagnostiquées positives ou à la liste des interactions sociales entre les personnes.*

  Bruno Sportisse (PdG INRIA)

- *Ça va nous aider à éviter le reconfinement et la propagation de l'épidémie*

  Cédric O

- *Un rapport sur le fonctionnement de StopCovid sera remis au plus tard le 30 janvier 2021*

  Décret du 29 mai 2020

Les promesses de StopCovid vs la réalité...

- *Sa conception permet que PERSONNE, pas même l'Etat, n'ait accès à la liste des personnes diagnostiquées positives ou à la liste des interactions sociales entre les personnes.*

  Bruno Sportisse (PdG INRIA)

  Vraiment ? !

- *Ça va nous aider à éviter le reconfinement et la propagation de l'épidémie* No comment...

  Cédric O

- *Un rapport sur le fonctionnement de StopCovid sera remis au plus tard le 30 janvier 2021*

  Décret du 29 mai 2020

  Date supprimée le 15 février 2021...

Privacy vis-à-vis du serveur

Sa conception permet que PERSONNE, pas même l'Etat, n'ait accès à la liste des personnes diagnostiquées positives ou à la liste des interactions sociales entre les personnes.

Bruno Sportisse (PdG INRIA), 18 avril 2020

- En cas de covid+, Alice remonte ses contacts, l'état a les moyens techniques de savoir qu'Alice est contaminée (adresse IP).
- L'état a également les moyens techniques de savoir qui Alice a recontré (graphe social).
- Si Bob est notifié à risque, l'état a les moyens techniques de savoir si Bob a continué à voir du monde (si Bob ou ses copains se déclarent positifs).

Privacy vis-à-vis du serveur

Sa conception permet que PERSONNE, pas même l'Etat, n'ait accès à la liste des personnes diagnostiquées positives ou à la liste des interactions sociales entre les personnes.

Bruno Sportisse (PdG INRIA), 18 avril 2020

- En cas de covid+, Alice remonte ses contacts, l'état a les moyens techniques de savoir qu'Alice est contaminée (adresse IP).
- L'état a également les moyens techniques de savoir qui Alice a recontré (graphe social).
- Si Bob est notifié à risque, l'état a les moyens techniques de savoir si Bob a continué à voir du monde (si Bob ou ses copains se déclarent positifs).

Of course, a State which is not a democratic State would have a very powerful tool for massive surveillance (even if it has much more efficient other tools) with a centralized approach.

Bruno Sportisse (PdG INRIA), 12 mai 2020

Utilisation des données à des fins policières

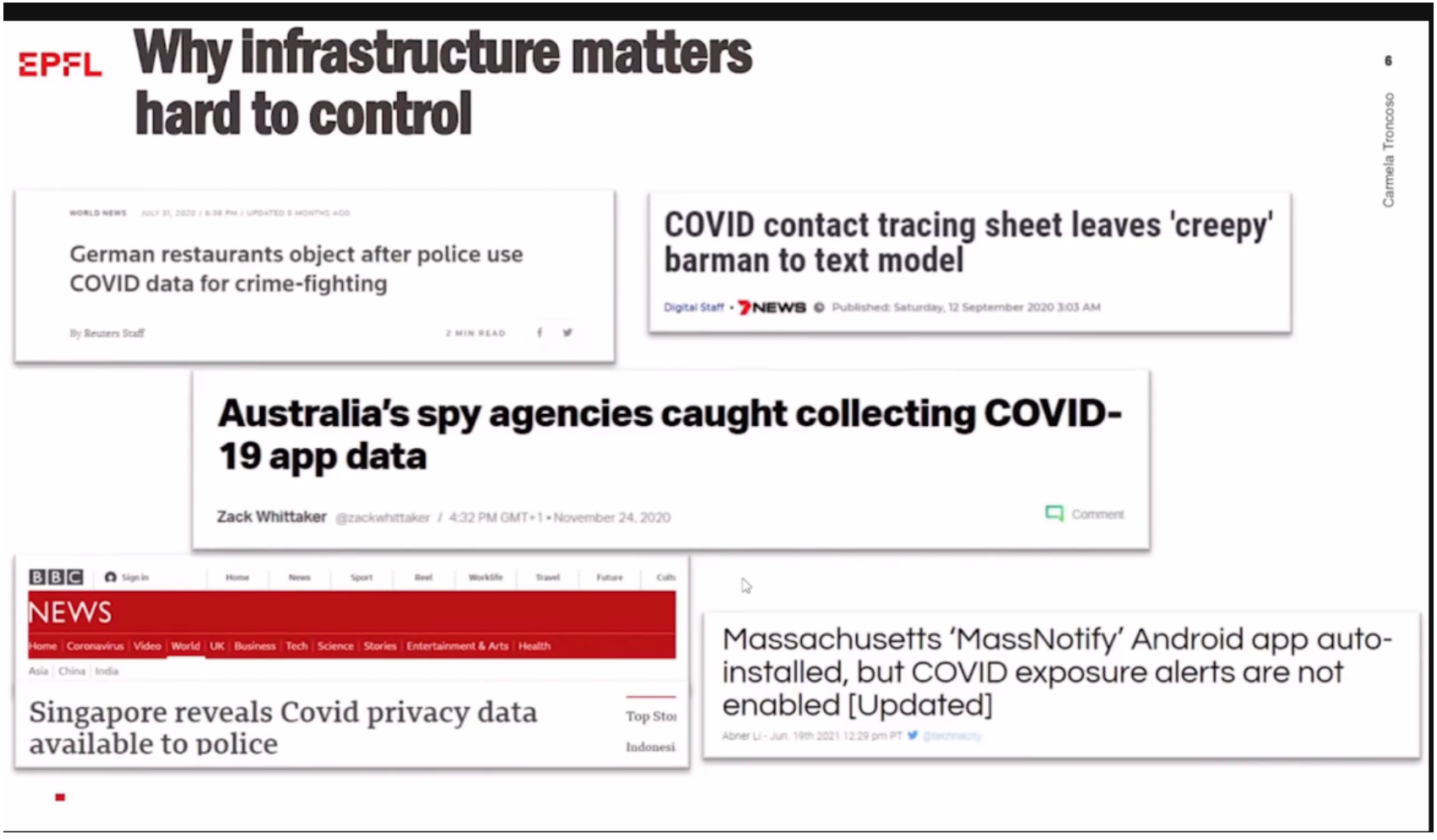


image empruntée à Carmela Troncoso (CSF 2021 invited talk)

Une solution possible : les mixnets

Plusieurs serveurs indépendants reçoivent chacun une partie des cas contacts et les mélangent avant de les remonter au serveur central

- Demande de la décentralisation...
- Difficile à mettre en pratique (délais, indépendance, ...)
- Jamais implémenté

Une solution possible : les mixnets

Plusieurs serveurs indépendants reçoivent chacun une partie des cas contacts et les mélangent avant de les remonter au serveur central

- Demande de la décentralisation...
- Difficile à mettre en pratique (délais, indépendance, ...)
- Jamais implémenté
- Pourtant l'impossibilité de remonter aux contacts est mentionnée par la CNIL *dans son avis*.

Questions pour le panel :

- La CNIL a-t-elle rendu son avis **en sachant** que les mixnets n'étaient pas implémentés ?
- La CNIL a-t-elle été mal informée par ses interlocuteurs notamment INRIA ?

Risques des applications de traçage

La privacy n'est pas garantie

Tous les systèmes de traçage permettent à un attaquant motivé de connaitre si les personnes avec qui il a été en contact ont été covid+

Risques des applications de traçage

La privacy n'est pas garantie

Tous les systèmes de traçage permettent à un attaquant motivé de connaitre si les personnes avec qui il a été en contact ont été covid+

- Un voisin motivé peut connaitre les personnes infectées de son immeuble
- Une organisation motivée peut le faire aussi, à plus grande échelle
- Suivant l'application : l'état et éventuellement Google/Apple peut savoir qui est infecté.

Risques des applications de traçage

La privacy n'est pas garantie

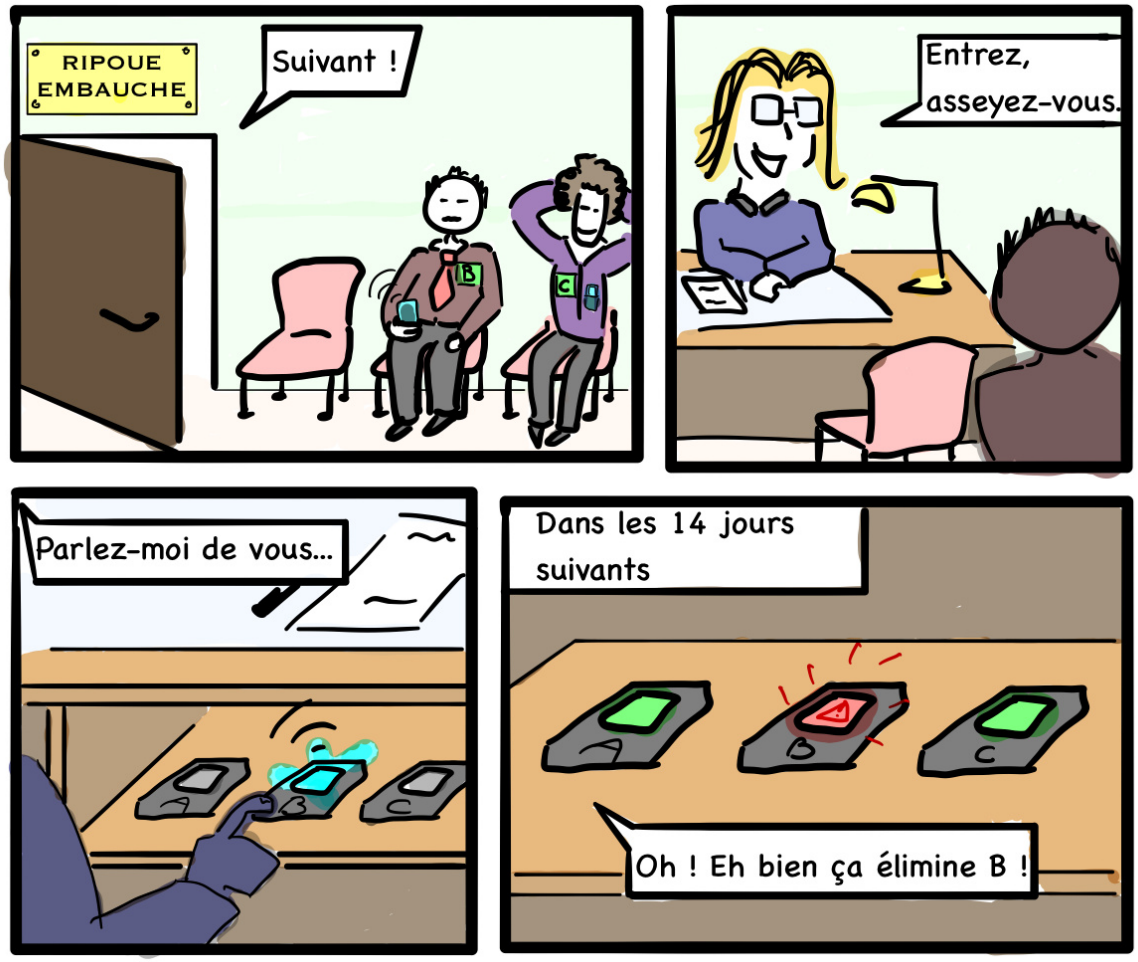
Tous les systèmes de traçage permettent à un attaquant motivé de connaitre si les personnes avec qui il a été en contact ont été covid+

- Un voisin motivé peut connaitre les personnes infectées de son immeuble
- Une organisation motivée peut le faire aussi, à plus grande échelle
- Suivant l'application : l'état et éventuellement Google/Apple peut savoir qui est infecté.

Fausses alarmes

Un attaquant peut provoquer des fausses alarmes en créant des "contacts" virtuels qui ne correspondent pas à une réelle proximité physique.

Le traçage anonyme, dangereux oxymore



Note : encore plus facile pour des applications type GAEN (pas besoin de téléphones dédiés)

En pratique : bugs et attaques

StopCovid :

- envoi de tous les contacts sans filtre de distance ni de durée
  - faille remontée par Gaëtan Leurent
  - repris par les médias (eg Le Monde)
  - mise en demeure publique de la CNIL
- champ `TxPower` en clair qui dépend du modèle de téléphone

StopCovid et GAEN :

- possibilité de relier les BLE à un identifiant global, en 10" d'attaque à 10m. *S&P'21*

En pratique : bugs et attaques

StopCovid :

- envoi de tous les contacts sans filtre de distance ni de durée
  - faille remontée par Gaëtan Leurent
  - repris par les médias (eg Le Monde)
  - mise en demeure publique de la CNIL
- champ `TxPower` en clair qui dépend du modèle de téléphone

StopCovid et GAEN :

- possibilité de relier les BLE à un identifiant global, en 10" d'attaque à 10m. *S&P'21*

GAEN

- Les logs de l'appli GAEN sont écrits dans les logs système, potentiellement envoyés lors de crash
- False notifications in Switzerland on iOS 13.7
- CoronaDetective : https ://www.coronadetective.eu/
  appli qui permet de lier les beacons BLE à des personnes

Pour quels bénéfices après un an ?

Maigres chiffres publics : #downloads et # notifications

- # downloads pas très pertinent (désinstallation, BLE pas activé, uniquement téléchargé pour le passe sanitaire)
- combien de notifications évidentes ? Combien de faux positifs ? (port du masque, cloisons, ...)

Pas d'étude terrain avec StopCovid

- StopCovid fonctionne mal :
  fully state-controlled apps such as StopCovid (FR) did have technical issues (excessive battery drain, having to run the app in the foreground, etc.) that are impossible to resolve.
  article signé par 10 auteurs dont C. Castellucia et V. Roca

Pour quels bénéfices après un an ?

Maigres chiffres publics : #downloads et # notifications

- # downloads pas très pertinent (désinstallation, BLE pas activé, uniquement téléchargé pour le passe sanitaire)
- combien de notifications évidentes ? Combien de faux positifs ? (port du masque, cloisons, ...)

Pas d'étude terrain avec StopCovid

- StopCovid fonctionne mal :
  fully state-controlled apps such as StopCovid (FR) did have technical issues (excessive battery drain, having to run the app in the foreground, etc.) that are impossible to resolve.
  article signé par 10 auteurs dont C. Castellucia et V. Roca

Il faut évaluer les bénéfices !

- une demande de nombreuses agences lorsqu'elles ont dû approuver la mise en place de l'application
- les risques (perte de privacy, fausses alarmes, attaques dues aux bugs) ne peuvent être acceptables qu'au regard des bénéfices reconnus

Et ça recommence : le pass sanitaire

Un QR-code signé, qui contient des infos perso :

- nom, prénom, date de naissance
- info de vaccination ou PCR
- obligatoire pour événements de 1000+ personnes, boites de nuit, pour les voyages

Et ça recommence : le pass sanitaire

Un QR-code signé, qui contient des infos perso :

- nom, prénom, date de naissance
- info de vaccination ou PCR
- obligatoire pour événements de 1000+ personnes, boites de nuit, pour les voyages

Comment vérifier la signature ? (version initiale)

- envoi à un serveur centralisé !
  - Le serveur sait qui utilise son pass sanitaire, quand et où
- infos qui transitent en clair par akamai (soumis au droit US)

Solution dont Inria est prestataire, validée dans l'avis de la CNIL

Et ça recommence : le pass sanitaire

Un QR-code signé, qui contient des infos perso :

- nom, prénom, date de naissance
- info de vaccination ou PCR
- obligatoire pour événements de 1000+ personnes, boites de nuit, pour les voyages

Comment vérifier la signature ? (version initiale)

- envoi à un serveur centralisé !
  - Le serveur sait qui utilise son pass sanitaire, quand et où
- infos qui transitent en clair par akamai (soumis au droit US)

Solution dont Inria est prestataire, validée dans l'avis de la CNIL

Est-ce qu'on ne sait pas faire mieux en 2021 en termes de privacy ?

Solution corrigée (?) suite à réaction des médias (e.g. MediaPart)

Quelles leçons ?

Notre communauté doit se définir des modalités pour travailler sous pression

- Les applis de traçage étaient une occasion en or de "faire quelque chose"
  $\rightarrow$ toute personne questionnant ces applis non bienvenue...
  $\rightarrow$ en quelques semaines, notre communauté a été coupée en deux, entre les "bons" et les "mauvais"

Quelles leçons ?

Notre communauté doit se définir des modalités pour travailler sous pression

- Les applis de traçage étaient une occasion en or de "faire quelque chose"
  $\rightarrow$ toute personne questionnant ces applis non bienvenue...
  $\rightarrow$ en quelques semaines, notre communauté a été coupée en deux, entre les "bons" et les "mauvais"

- De la politique plutôt que de la science
  - Les gouverments devaient faire "quelque chose"
  - Les compagnies privées sont très intéressées par les données personnelles médicales
  - Les organismes de recherche (e.g. Inria) souhaitaient gagner en visibilité
    $\rightarrow$ critiquer stopcovid est un acte de traitrise

Quelles leçons ?

Notre communauté doit se définir des modalités pour travailler sous pression

- Les applis de traçage étaient une occasion en or de "faire quelque chose"
  $\rightarrow$ toute personne questionnant ces applis non bienvenue...
  $\rightarrow$ en quelques semaines, notre communauté a été coupée en deux, entre les "bons" et les "mauvais"

- De la politique plutôt que de la science
  - Les gouverments devaient faire "quelque chose"
  - Les compagnies privées sont très intéressées par les données personnelles médicales
  - Les organismes de recherche (e.g. Inria) souhaitaient gagner en visibilité
    $\rightarrow$ critiquer stopcovid est un acte de traitrise

Pression sur les concepteurs d'application pour produire un protocole très vite, sans évaluation par les pairs
Pression sur les détracteurs pour ne pas parler à la presse

Pour conclure

- Nous avons besoin de faire mieux, en tant que communauté scientifique
- Comment les bénéfices des applications sont évalués à l'heure actuelle ?
- Sur le long terme, souhaite-t-on encourager les applications de traçage / surveillance, pour des raisons médicales ?