Think Data

Principles: Safety and security, Fairness and non-discrimination, Privacy, Transparency and explainability, Responsibility and accountability, Multi-stakeholder and adaptive governance and collaboration
Values: Human Rights , Ensuring diversity and inclusiveness, Living in harmony and peace
Stakeholders: Civil society, Public sector, Media, Academia, Technical community

Anti Covid platform's side effects on privacy and security of users

Due to the current COVID pandemic, a government decides to launch a mobile application to detect infections by geolocating infected users and notifying their contacts. The application is developed by a special commission that has the mission of creating the most efficient application without endangering the rights of the users.

Users download the application and register by creating pseudonyms so that their profile remains anonymous. The application functions with Bluetooth to locate users and then send's notifications if they came across a sick person. The platform traces the user's movements and stores them in the system.

However, the application is flawed and puts at risk its users for various reasons. The application encourages a new form of "witch hunt" for infected cases. Even though the application uses pseudonyms, it is easy for people to retrace their interactions and spot the one who contaminated them, sometimes wrongly. This is particularly dangerous in for people from certain origins or jobs who can be wrongly accused. Furthermore, the use of Bluetooth is also on itself a security risk for the users. One of the flaws of Bluetooth is that when activated it gives access to other people, some of which mal intended, to personal private information. Moreover, the information gathered by the application can also be used by private companies with the goal to profit from them. Lastly, the fact of tracing the individuals on itself poses a threat to their privacy and security.

The application is removed from download platforms and is reviewed by the commission.

When working on sensitive information that touches people's lives directly, it is important to understand all the challenges and problems that can appear from such practice. Being transparent and reassuring the people on how their information is dealt with is essential as it will increase their trust in you and in the application therefore gaining more users and being able to have a real effect.

How could this situation have been avoided in the first place?

Here are our recommendations per stakeholder:

- Developers and engineers strengthen the security parameter of the application so that the data collected is only accessible by the Commission. They also switch for geolocation rather than Bluetooth. They also include a new option, "Authorize my tracking" so that people can chose when they are tracked.

- The Commission after updating the application, makes sure that a protection of the data legislation is passed to protect the user's information. Data is only used by the commission and to do so, workers have to follow a very strict protocol.

- Users are asked to stop "witch hunting" for sick people and encouraged to download the application for better results.

- The Government launches awareness campaigns to educate people on hygiene measures as to prevent the propagation of the virus and invests in the medical system as to have enough care for all.

Privacy & Human Rights & Responsibility and accountability & Safety and security & Proportionality and do no harm & Fairness and non-discrimination

Know more about this case:

- «Les risques de StopCovid» (The risks of StopCovid), Le Figaro, https://www.lefigaro.fr/secteur/high-tech/les-risques-de-stopcovid-20200413

- "Le traçage anonyme, dangereux oxymore Analyse de risques à destination des non-spécialistes" (Anonymous tracing, a dangerous oxymoron Risk analysis for non-specialists), https://risques-tracage.fr/docs/risques-tracage.pdf

Related work:

- "S Korea's smartphone apps tracking coronavirus won't stop buzzing", Al Jazeera, https://www.aljazeera.com/news/2020/4/9/s-koreas-smartphone-apps-tracking-coronavirus-wont-stop-buzzing

- "Major Security Flaws Found in South Korea Quarantine App", The New York Times, https://www.nytimes.com/2020/07/21/technology/korea-coronavirus-app-security.html

- "South Korea is relying on technology to contain COVID-19, including measures that would break privacy laws in the US — and so far, it's working", Business Insider, https://www.businessinsider.com/coronavirus-south-korea-tech-contact-tracing-testing-

fight-covid-19-2020-5?IR=T

- "Coronavirus mobile apps are surging in popularity in South Korea",
  CNN, https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html

- "Designing an app to combat COVID-19 in Germany",
  PWC, https://www.pwc.com/gx/en/about/case-studies/covid-19-tracking-app-case-study-germany.html

- "TraceTogether: Singapore turns to wearable contact-tracing Covid tech",
  BBC, https://www.bbc.com/news/technology-53146360