Mobile usage during COVID-19

Created by: Rebeka Szűcs and Dóra Maros PhD

Keywords: data protection, privacy, mobile application security, COVID-19

Introduction

- Mobile & Internet era: growing number of users
- Smartphones can also help in crisis situations like this pandemic
- Coronavirus 2 (SARS-CoV2), a serious acute respiratory syndrome that appeared at the end of 2019, and the disease it causes, coronavirus disease 2019, abbreviated as COVID-19
- The purpose of this presentation is to summarize and review the use of mobile devices during the COVID-19 pandemic, including issues related to security, data protection and privacy, as this new situation presents new opportunities but also new risks.

MOBILE PHONE USAGE DURING COVID-19

- **Contact tracing**: Practically means that the infected patient is questioned with whom they have spent more time in the recent period (in this case about two to three weeks), with whom they have had close contact, as these people are more likely to have caught the virus
  - Apps use Bluetooth to track nearby, lengthier contacts between users, it records them, and then notify users who have recently contacted each other (anonymously) if an infection is confirmed
  - First was TraceTogether (Singapore)
- **Quarantine monitoring**
- **Apps that monitor the condition and recovery** of patients at home
- **Information apps**

Concern: storage and data processing

- **Decentralized**: personal data as well as the identifiers generated by the application remain on the user's mobile phone
- **Centralized**: in which the application works through a managed background server owned by the national public health organisation. The identifiers are stored and paired there
- According to the EU recommendation, both solutions could be combined with, for example, voluntary data sharing, i.e. if the user is positive, he or she can enter and voluntarily send data to the central database for further analisys
- Additional functions can be integrated into any solution as well, through which the user can even receive information and help about the disease from the authorities

Privacy and security concerns

- Surveillance capitalism and surveillance creep- apps are associated with mass surveillance, important topic to address
- New forms of cybercrime tailored to COVID
  - Crimes in the name of WHO or country health ministries to steal personal data
  - Attacks against hospitals with weak security (ransomware)
  - Collecting money in the name of public health agencies
  - Fraudulent apps and websites which steal data/ infect devices with malware
  - Attacks on online meeting apps
- Conspiracy theories

Thank you for your attention