NIEDERER KRAFT FREY

COVID-19 CT Apps on the rise: What are the privacy concerns?

IAPP virtual Switzerland KnowledgeNet Chapter Meeting

Zurich — 27 April 2020

Table of Contents

1. Introduction
2. Example: Swiss DP-3T CT App
3. Data Protection, technical and other Challenges
4. Conclusions

Introduction

Introduction

Source: Keystone /Darren England

Role of CT Apps in Combat of COVID-19

- Monitoring and mitigating ongoing COVID-19 pandemic
- Facilitate organisation of medical follow-up
- Provide direct guidance to citizens
- Automatisation of contact tracing and warning
- Research

DISTANCE TRACKING... V2.0
SEPT.19.2020: 05:17
PROGRESS..... 65 OBJECTS.....9 CRITICAL.....21 WARINGS.....ON HOLD.....05:12......12 OBJECTS......1 CRITICAL

CT App Frameworks

- Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)
- Google / Apple privacy-preserving tracing project
- Decentralized Privacy-Preserving Proximity Tracing (DP-3T)
- BlueTrace / OpenTrace
- TCN Coalition / TCN Protocol
- The promoters are mainly governments (China, Singapore), but also institutions (e.g. Robert Koch Institute, Fraunhofer Institute for telecommunications), universities (EPFL, ETHZ, University Colleage London) and foundations (ITO, Zcash Foundation, etc.)

CT Apps in Use and Contemplated

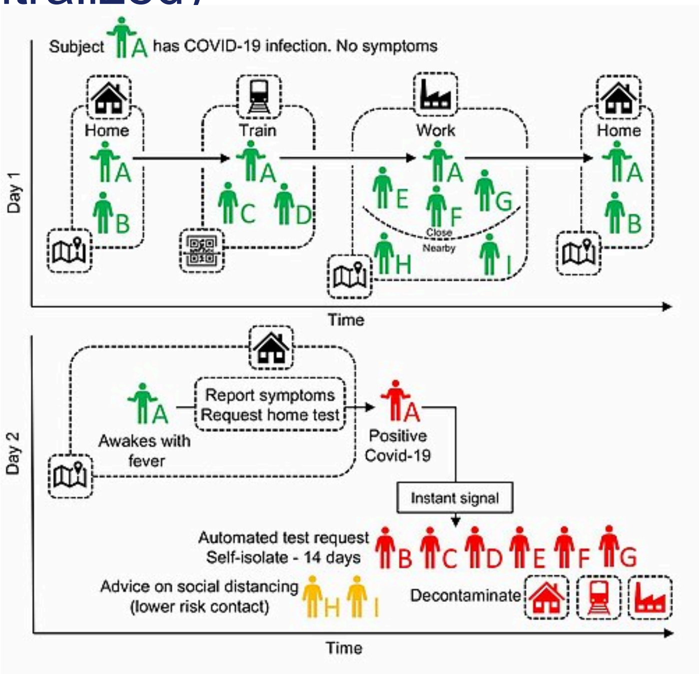
- Countries with official Apps in current use:
  - China: Alipay Health Code (proprietary)
  - Singapore: Trace Together (protocol: BlueTrace)
  - Norway: Smittestopp (proprietary)
  - Israel: Hamagen (MIT license)
  - Etc.
- Countries considering deployment:
  - Austria: Stopp Corona (protocol: DP-3T)
  - Switzerland: under development (protocol: DP-3T)
  - Russia: under development

Hubei, Mainland China

Confirmed	Recovered	Deaths
67,592	42,033	2,931

Technologies used in CT Apps

- Mobile software applications designed to aid contact tracing in response to COVID-19 combat, i.e. the process of identifying persons ("contacts") who may have been in contact with an infected individual
- GPS tracking technologies (centralized)
- Bluetooth technologies (decentralized)
- Differences Eastern (personal and identifiable data) and Western (anonymized and aggregated data) countries



Example: Swiss DP-3T App

Swiss DP-3T App

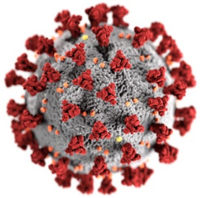
- Decentralized Privacy-Preserving Proximity Tracing system downloadable onto smartphones developed by Switzerland’s two Federal Institutes of Technology (ETHZ and EPFL)
- ETHZ and EPFL pulled out of PEPP-project: dispute over centralized vs. decentralized systems
- Employs Bluetooth Low Energy (LE) technology to allow smartphones to communicate with each another anonymously (e.g. like headphones connecting to smartphone)
- No need for localization of mobile smartphones, hence no localization/GPS data necessary
- DP-3T App is designed to record when two people come near one another without revealing their identities or location

How does Swiss DP-3T App work? I

- **Installation:** installed DP-3T App generates a secret key (SK) which is daily rotated and creates Ephemeral Bluetooth IDs (EphIDs) (=Bluetooth Low Energy beacons)
- **Normal operation:** each DP-3T App broadcasts EphIDs via bluetooth and records all EphIDs that are broadcast by other mobile smartphones in the vicinity
- **Handling infected patients:** after patients are diagnosed and only with their consent and with authorization from a health authority, they upload specific data from phone to the backend server. From this data the identity of the patient cannot be derived by the server or the DP-3T Apps of the other users, it is (nearly) anonymous. Before this point no data other than the broadcast EphIDs leaves the phone

How does Swiss DP-3T App work? II

- **Decentralized contact tracing:** each DP-3T App can use data from the backend to locally compute whether the DP-3T App's user was in physical proximity of an infected person and potentially at risk of an infection. If they were, the DP-3T App can inform the user to take action
- **Voluntary provision of data for research:** in addition the user can voluntarily provide anonymous data for epidemiology research centers



When two people are near each other, their phones can exchange an anonymous identification key, recording that they've had close contact. No name, location or other personal data is necessary

NKF

Swiss DP-3T CT App – Graphics I

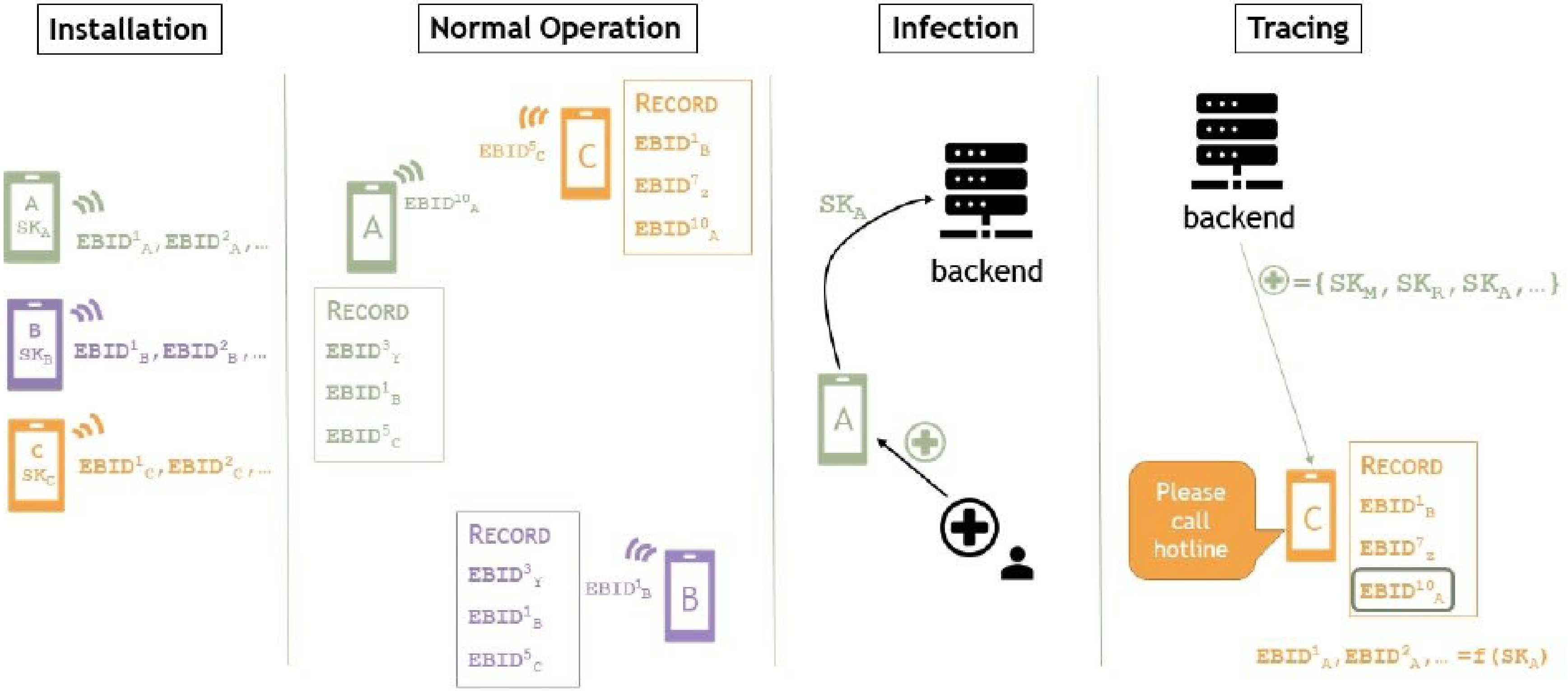


Figure 1: Phases in the decentralized proximity tracing system

Swiss DP-3T CT App – Graphics II

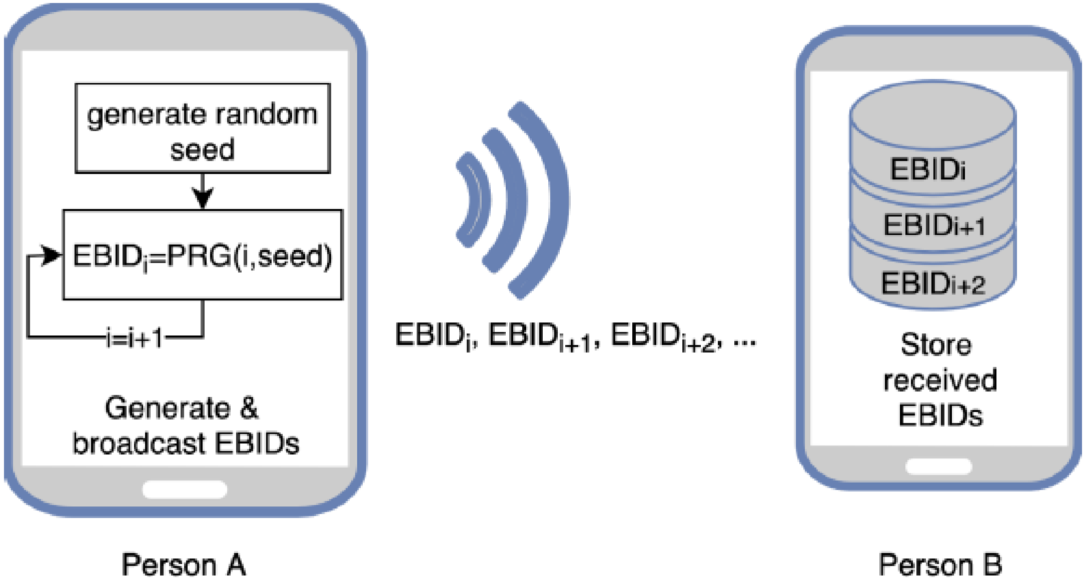


Figure 2: Generation and broadcasting of ephemeral identifiers/EphIDs

Swiss DP-3T CT App – Graphics III

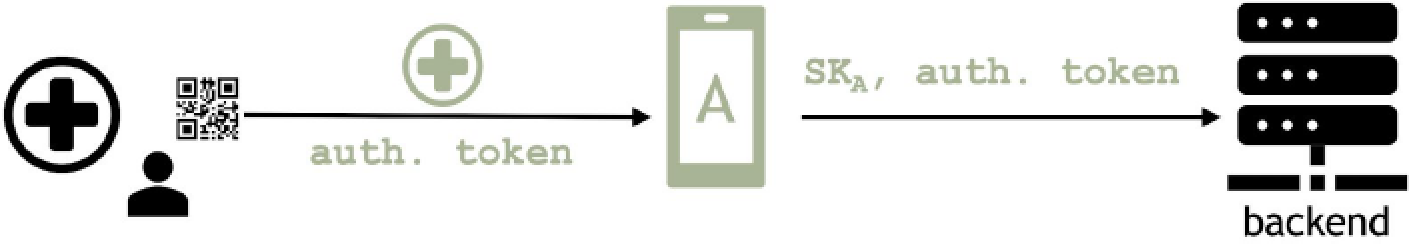


Figure 3: Information by infected patient

NKF

Swiss DP-3T CT App – Graphics IV

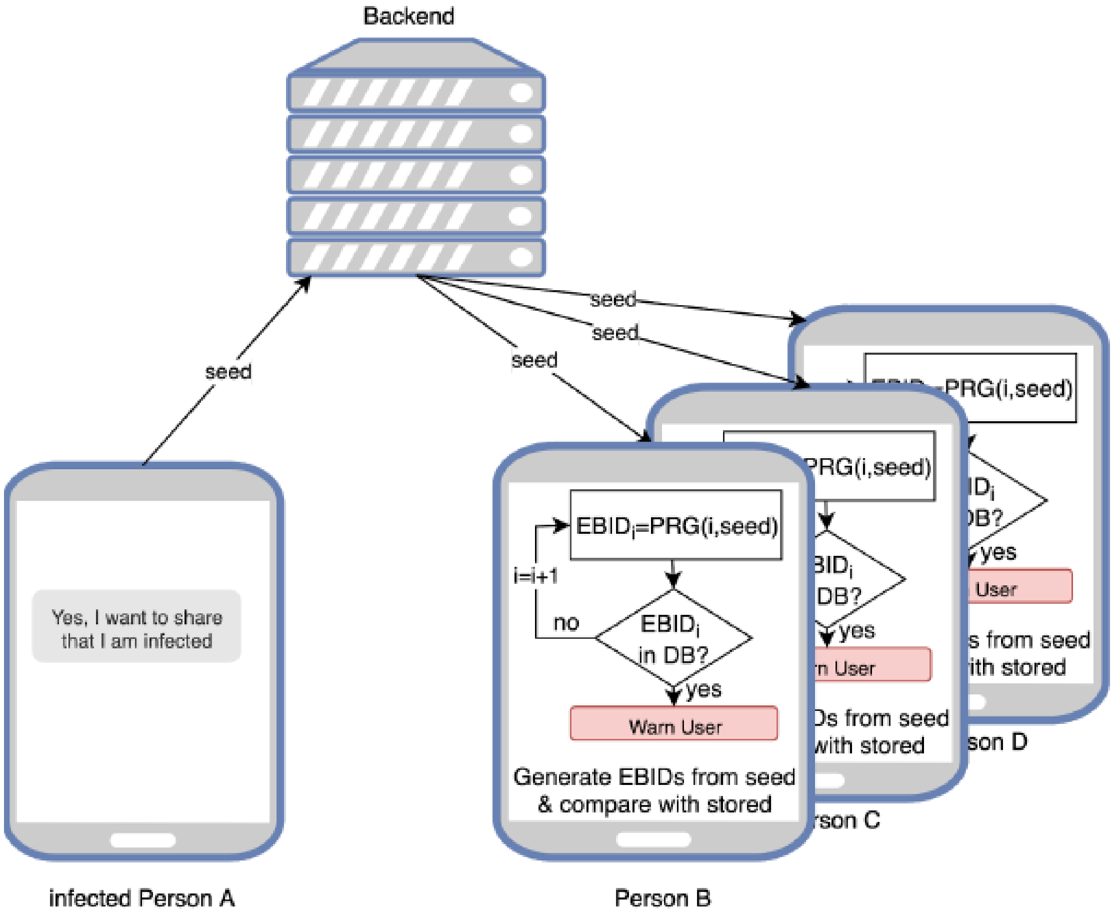
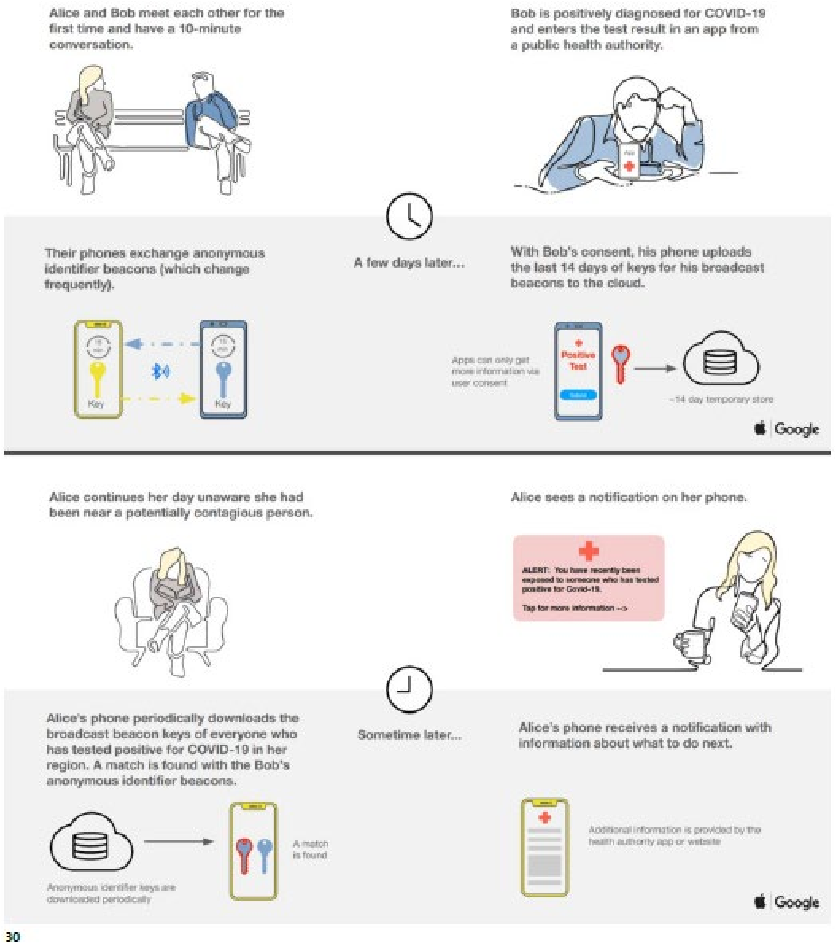


Figure 4: Warning of persons at risk

Or put in more simple terms….



Alice and Bob meet each other for the first time and have a 10-minute conversation.

Their phones exchange anonymous identifier beacons (which change frequently).

A few days later...

Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.

With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

Alice continues her day unaware she had been near a potentially contagious person.

Alice's phone periodically downloads the broadcast beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with the Bob's anonymous identifier beacons.

Sometime later...

Alice sees a notification on her phone.

ALERT: You have recently been exposed to someone who has tested positive for Covid-19.

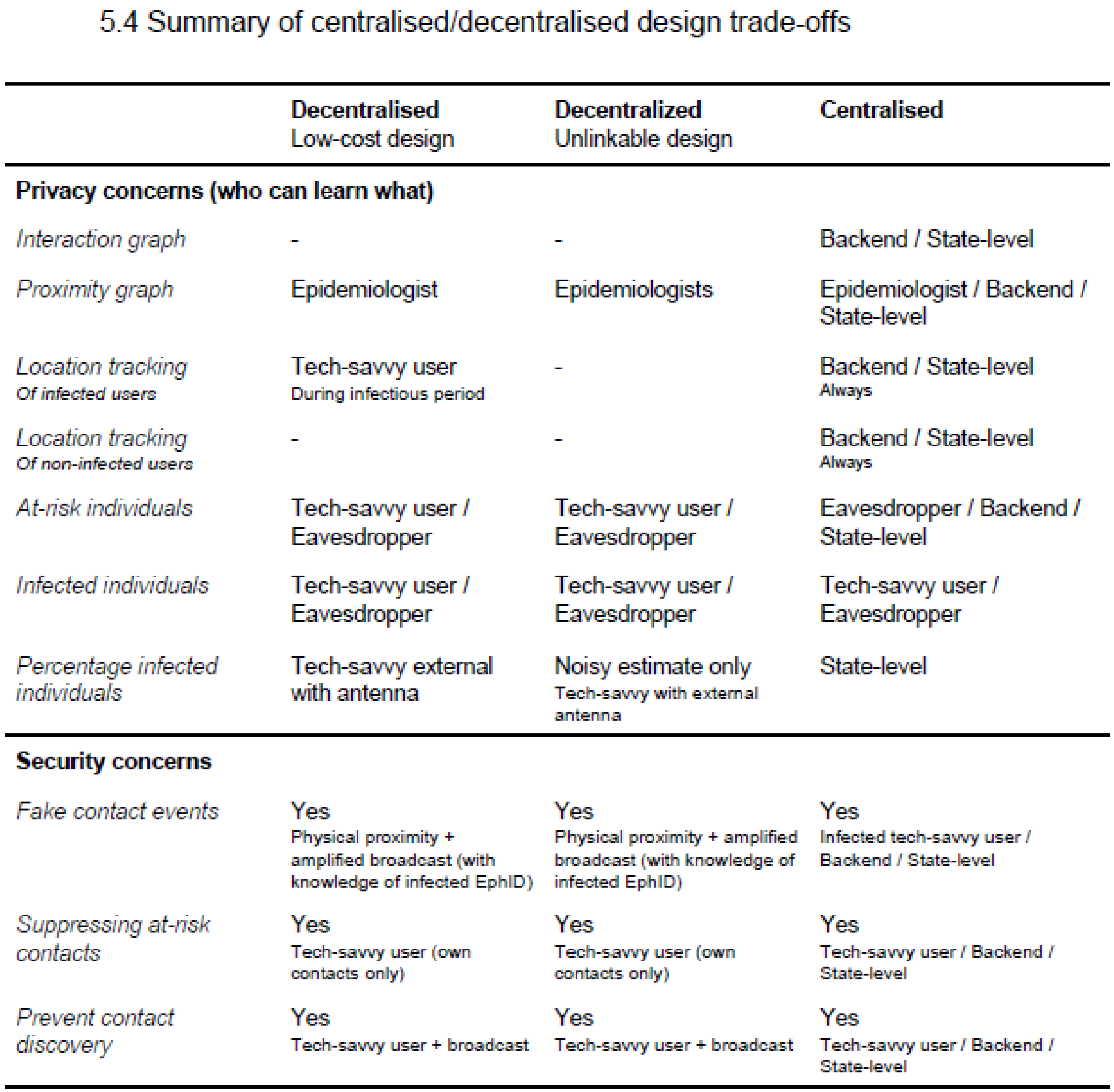
Tap for more information -->

Alice's phone receives a notification with information about what to do next.

Additional information is provided by the health authority app or website
Google

30

Centralized vs. Decentralized Designs



5.4 Summary of centralised/decentralised design trade-offs

	Decentralised Low-cost design	**Decentralized** Unlinkable design	**Centralised**
Privacy concerns (who can learn what)			
Interaction graph	-	-	Backend / State-level
Proximity graph	Epidemiologist	Epidemiologists	Epidemiologist / Backend / State-level
Location tracking *Of infected users*	Tech-savvy user During infectious period	-	Backend / State-level Always
Location tracking *Of non-infected users*	-	-	Backend / State-level Always
At-risk individuals	Tech-savvy user / Eavesdropper	Tech-savvy user / Eavesdropper	Eavesdropper / Backend / State-level
Infected individuals	Tech-savvy user / Eavesdropper	Tech-savvy user / Eavesdropper	Tech-savvy user / Eavesdropper
Percentage infected individuals	Tech-savvy external with antenna	Noisy estimate only Tech-savvy with external antenna	State-level
Security concerns			
Fake contact events	Yes Physical proximity + amplified broadcast (with knowledge of infected EphID)	Yes Physical proximity + amplified broadcast (with knowledge of infected EphID)	Yes Infected tech-savvy user / Backend / State-level
Suppressing at-risk contacts	Yes Tech-savvy user (own contacts only)	Yes Tech-savvy user (own contacts only)	Yes Tech-savvy user / Backend / State-level
Prevent contact discovery	Yes Tech-savvy user + broadcast	Yes Tech-savvy user + broadcast	Yes Tech-savvy user / Backend / State-level

Data Protection Challenges

Swiss DP-3T App and Data Protection

- ETHZ and EPFL’s views on DP-3T App and data protection:
  - **No personal data transmitted:** the risk model transmitted is not individual and therefore not personal data
  - **No personal data on the server:** data held on server cannot be linked to individuals during normal operation. The user upon downloading this non-personal data computes a new category of personal data locally on their devices: their risk score(s)
  - **Data only on device of user:** the data used to compute the risk score is held only on the device of the user
  - **Opt-in to send to epidemiology centers:** if the user opts-in to sending this data for epidemiologic research, the data they can send contains few variables and no identifier among them. Hence no personal data in the hands of the researchers

Concerns and Challenges I

- Are the secret key (SK) and the derived Ephemeral Bluetooth IDs (EphIDs) from it, actually considered not to be personal data?
- What is an EphID?
  - BLE Beacons = small bluetooth radio transmitters
  - It transmits a unique ID number that tells a listening device which beacon it's next to
  - The beacon sends out its ID numbers about ten times every second
  - A nearby Bluetooth-enabled device, like a mobile smartphone, picks up that signal
  - A dedicated app recognizes it, it links it to an action or piece of content stored in the cloud and displays it to the user
  - Ephemeral means: the ID changes every few minutes

Concerns and Challenges II

- Most likely EphID is not considered to be personal data since not every theoretical possibility of identification or singularisation is enough
- Accordingly data protection laws do not apply!
- However still concerns:
  - How can anonymization be ensured?
  - How can encryption be ensured?
  - How are secret key (SK) and Ephemeral Bluetooth IDs (EphIDs) created and exchanged?
  - Can eavesdropping operations be excluded or prevented?
  - How much data and what kind of data shall be transmitted to the backend server?

Concerns and Challenges III

- Answer from EDPB on 21 April 2020
- EDPB Guidelines 04/2020 on location data and contact tracing tools:
  - *Legal basis:* use of CT Apps should be voluntary
  - *Location tracking:* not necessary
  - *Data storage and controllership:* should be decentralized
  - *Warning individuals:* app developers should work closely with health authorities; CT Apps need to contain strong anonymization features
  - *Algorithms*: used in CT Apps should work under strict supervision of qualified personnel
  - *Data retention:* collected data to be anonymized and erased after COVID-19

Technical Challenges

Technical Challenges

- Bluetooth technology is being converted to measure distances
- CT App / smartphone device sends out radio signals and also listens out for such signals
- Depending on the strength of the signal, the distance can be assessed
- Large source for false or inaccurate information:
  - Glass pane: bluetooth radio signals can pass through: cyclist next to car…
  - How long do devices have to be in proximity to each other?
  - EphID are only kept for 14 days on the smartphone
  - Smartphone battery is dead, etc.

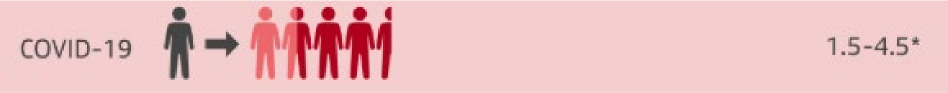
Other Challenges

Other Challenges I

- Critical mass needed using the CT Apps in order for them to work
- Does voluntariness work?
  - Who will install the CT App? It has to happen voluntarily or then a law is required imposing this on the population
  - Will a user voluntarily report his/her positive COVID-19 test – even if he/she has very mild symptoms?
  - Will an alerted user stay voluntarily in quarantaine?
  - Or do only state ordered systems like in China and South Korea work properly?
- Further questions:
  - Does the implementation and use of CT App require a legal basis / the enactment of a law?

Other Challenges II

- Do the CT Apps have to be authorized and by whom?
- Who sets and approves the technical requirements?
- How reliable is the CT App?
- How long shall CT Apps be used?
- When shall the collected data be deleted?
- How to handle banter or false alerts?
- Etc.



Conclusions

Conclusions

- Data protection is not the main problem – rather other factors
- CT Apps do not replace traditional contact tracking interviews
- Swiss Parliamentary Commission requests that a legal basis / a law is enacted
- Many experts – many providers – many different views
- Most likely decentralized CT App like the Swiss DP-3T App will be acceptable for many citizens
- However, citizens do not want to be tracked and monitored…
- Concept of voluntariness does most likely not work – critical mass of users will not be reached (50%-70%)
- Success of DP-3T App will depend on whether the use of it is mandatory and enforced by Swiss State

THANK YOU

Questions?

Clara-Ann Gordon
clara-ann.gordon@nkf.ch
D +41 58 800 84 26

NKF