

DP3T

Distributed privacy- preserving contact tracing

April 13th, 2020

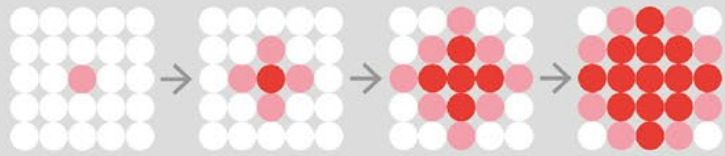
- Since the DP3T protocol is evolving quickly, please always check with authors for the latest materials, checking the date on the title page.
- The most recent information on the project and contacts are available at <https://github.com/DP-3T/documents>

How can contact tracing help?

As far as COVID-19 cares, there are 3 kinds of people:

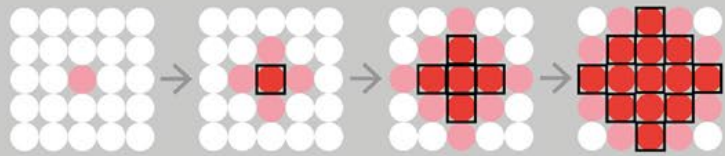


If we do nothing



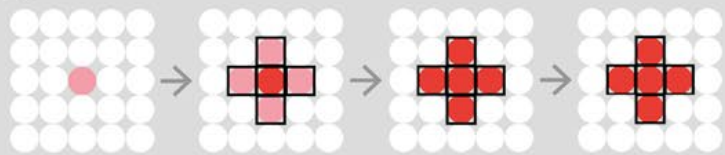
We get a wave of infections

If someone finds out they're infected, they immediately self-isolate:

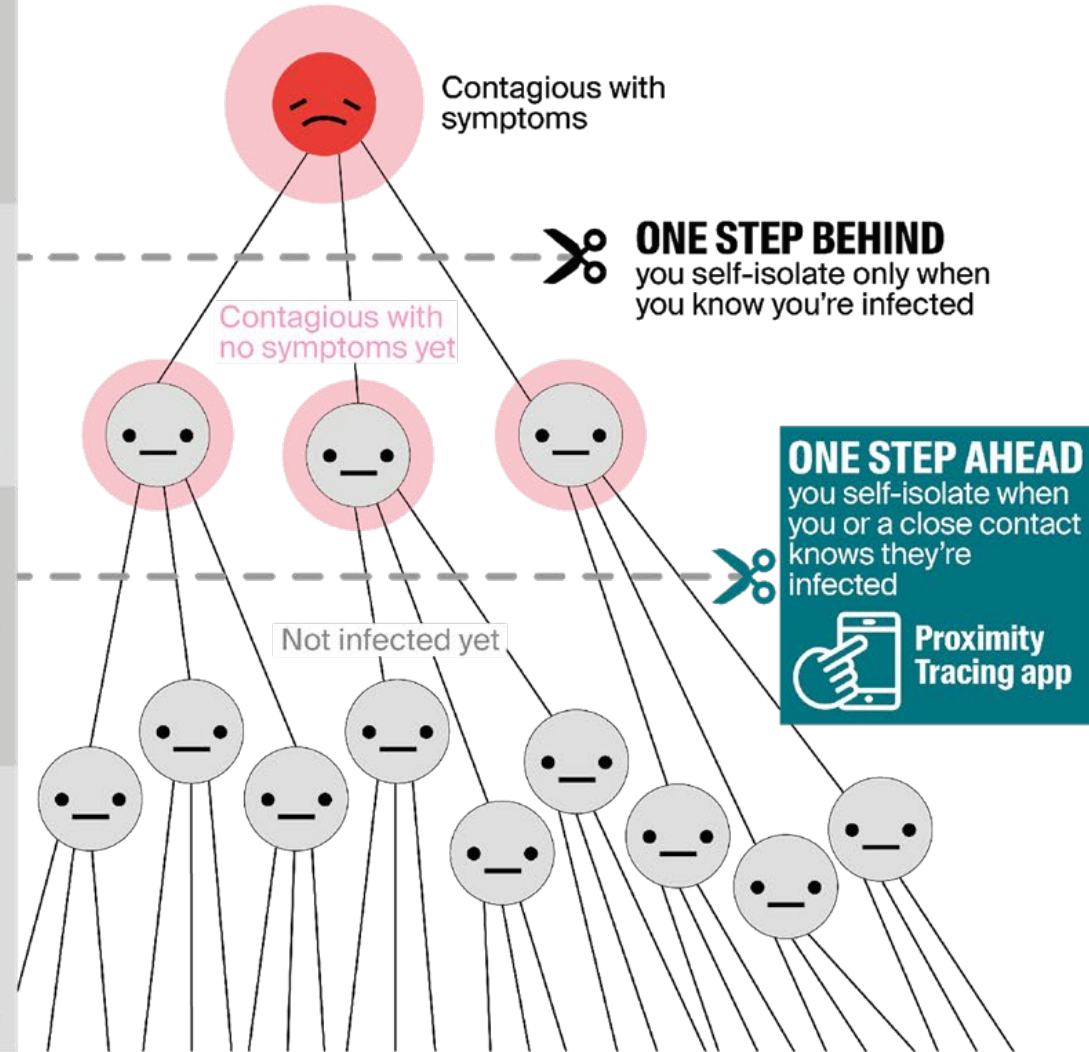


We are one step behind the virus

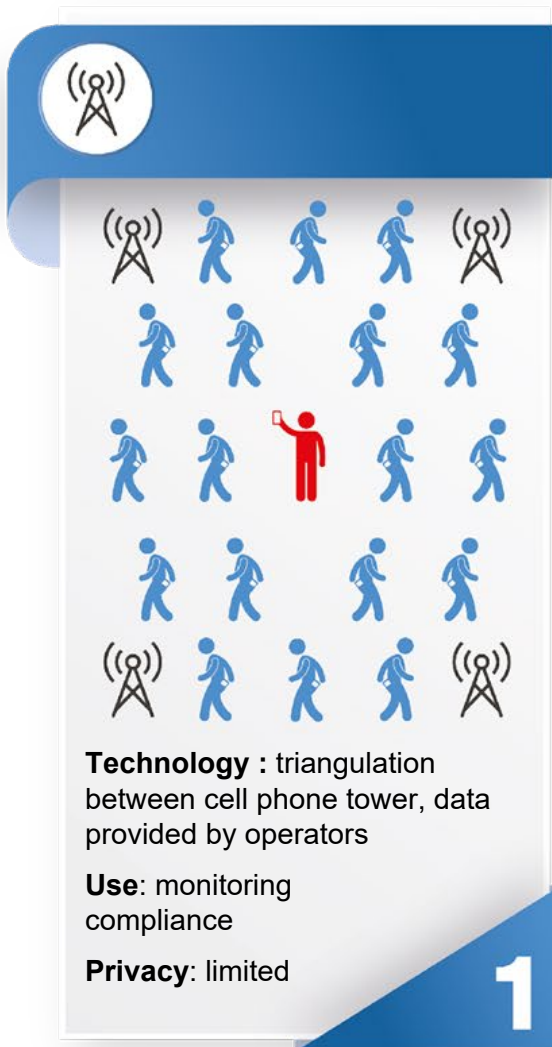
If someone finds out they're infected, they and their close contacts self-isolate



We are one step ahead



Three scenarios for contact tracing

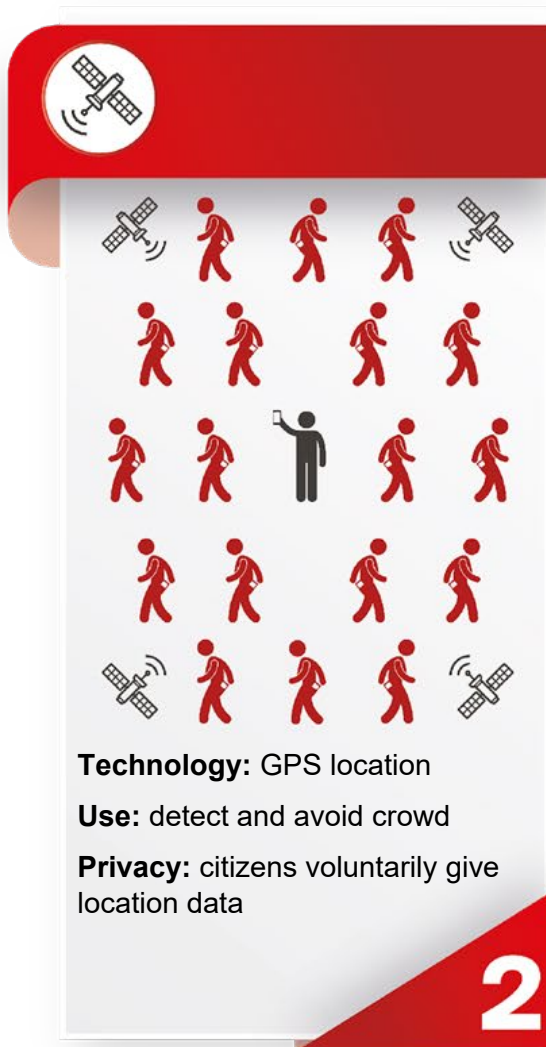


Technology : triangulation between cell phone tower, data provided by operators

Use: monitoring compliance

Privacy: limited

1

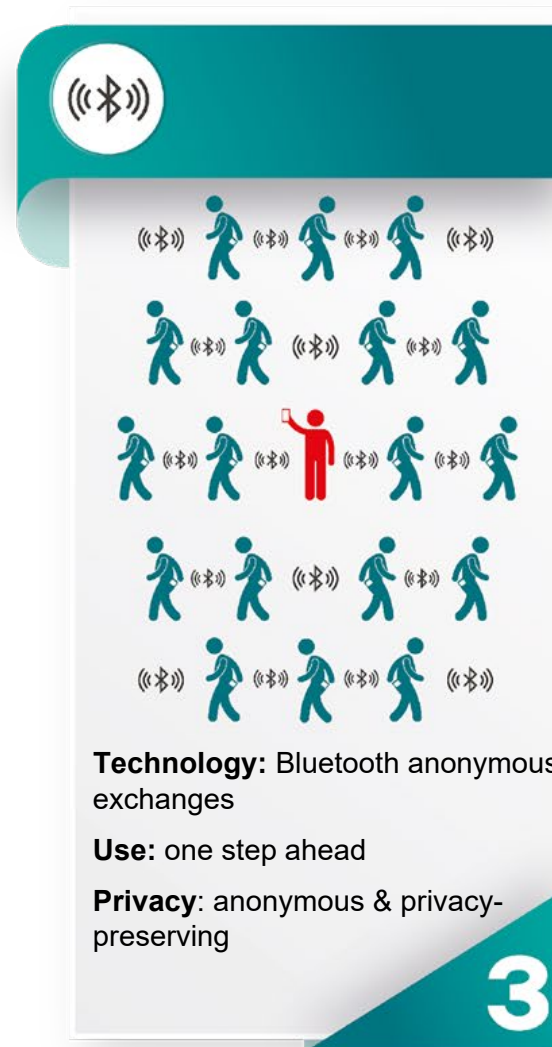


Technology: GPS location

Use: detect and avoid crowd

Privacy: citizens voluntarily give location data

2



Technology: Bluetooth anonymous exchanges

Use: one step ahead

Privacy: anonymous & privacy-preserving

3

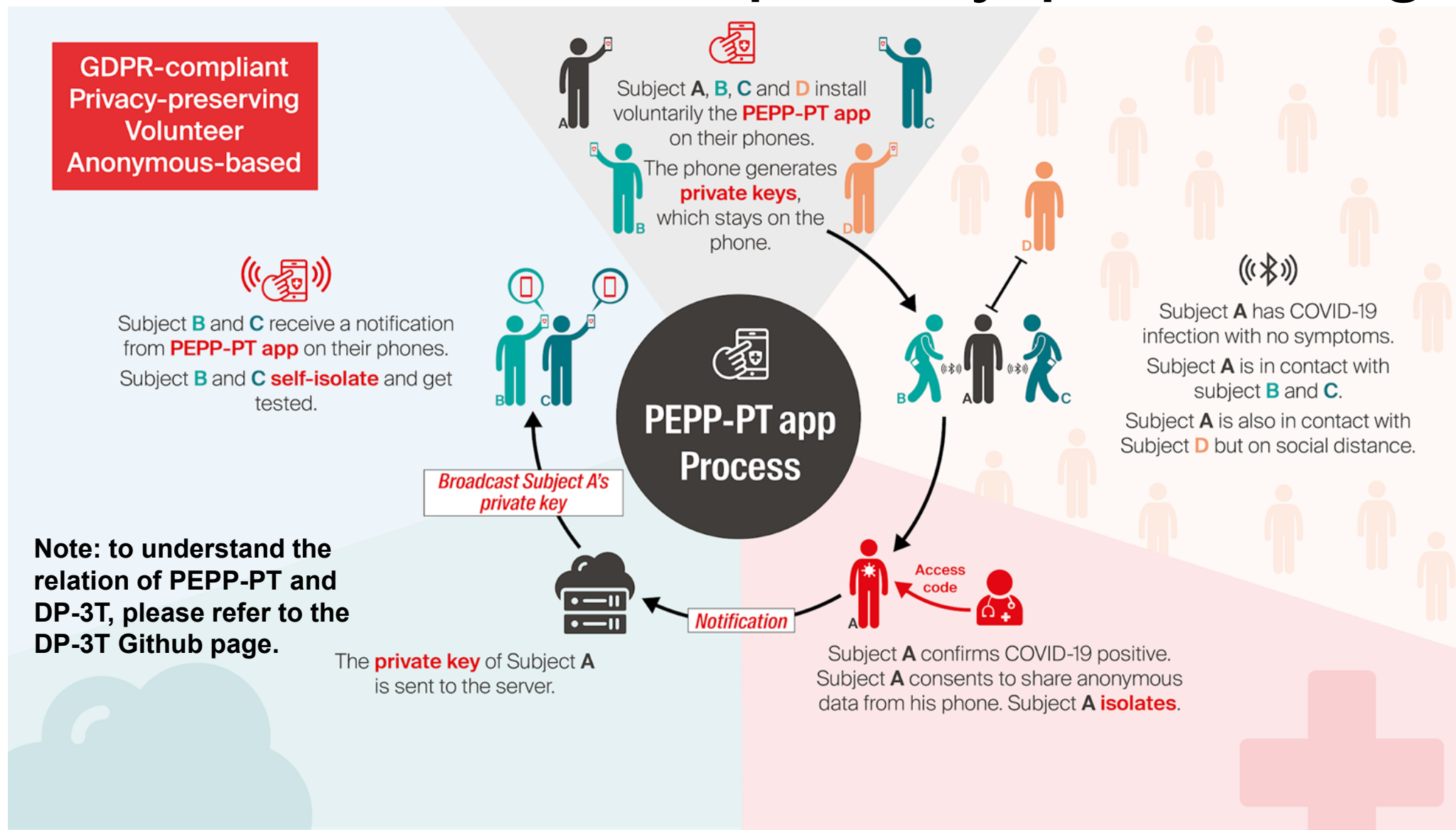
Goals to be solved by the application

- 1) People are quickly informed that they may have been in contact with a person infected with SARS-CoV-2.
- 2) After contact, the person receive instructions on which further actions to take (this part is country-specific).
- 3) Epidemiologists receive anonymous or pseudonymous research information about the spread of SARS-CoV-2 from volunteering users.

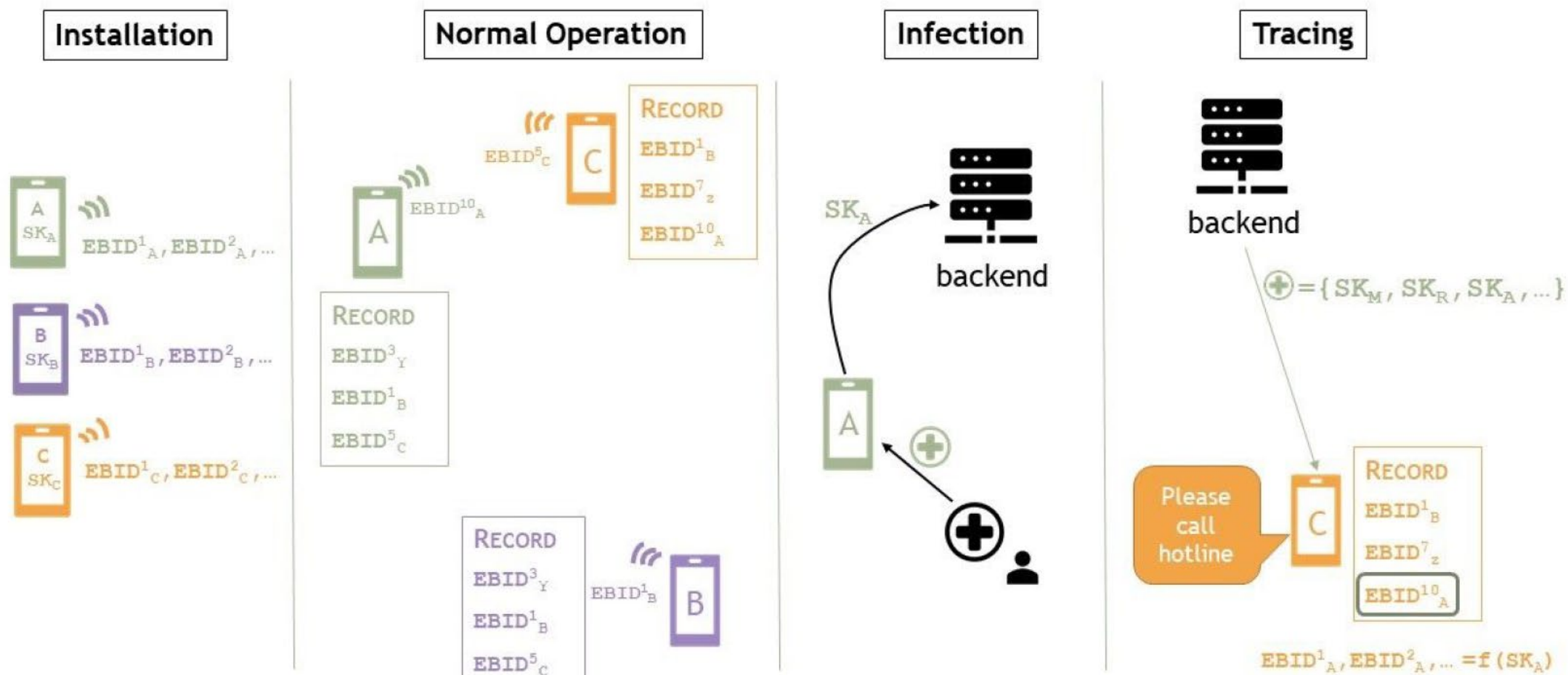
Security and privacy goals

- 1) The system can not be used to track healthy individuals.
- 2) The data processing has been minimized, but goals are still reached.
- 3) Data abuse is avoided using technical measures.
- 4) The system scales to countries with millions to hundreds of millions of people.
- 5) The system is compatible with as the most common mobile phones.
- 6) Joining the system is voluntary.

DP-3T is distributed, privacy-preserving



Bluetooth + ephemeral identifiers



Comparison of distributed vs centralized

	Decentralized	Centralized
Interaction graph	-	Backend / State-Level
Proximity graph	Epidemiologist	Epidemiologist / Backend / State-Level
Location tracking: infected users	Tech-savvy user (during infection)	Backend / State-Level (always)
Location tracking: non-infected users	-	Backend / State-Level (always)
At-risk individuals	Tech-savvy user / Eavesdropper	Eavesdropper / Backend / State-Level
Infected individuals	Tech-savvy user / Eavesdropper	Tech-savvy user / Eavesdropper
Percentage infected individuals	Tech-savvy external with antenna	State-Level

Comparison of specific risks

	Decentralized	Centralized
Fake contact events	Physical proximity + amplified broadcast	Infected tech-savvy user / Backend / State-Level
Suppressing at-risk contacts	Tech-savvy user (own contacts only)	Tech-savvy user / Backend / State-Level
Prevent contact discovery	Tech-savvy user + broadcast	Tech-savvy user / Backend / State-Level

The backend has two main components



Health System IT infrastructure
(see assumptions)

Case management

Medically-regulated environment
(may have its own mobile health app)

DP3T Infrastructure

Anonymous

Not medically regulated

Pan-European exchanges for
roaming purposes

Providing data to epidemiologists

- During application setup, the user can opt in to sharing data with epidemiologists.
- If the user opts in:
 - Every day, a dummy packet of data is sent to avoid detecting infection through traffic analysis.
 - On the day of infection, should that come, the user gets to confirm whether to share data or not.
 - If yes, data is shared with the designated agency in pseudonymous form, allowing for a construction of the infection graph.

DP3T team (list is updated constantly)

- **EPFL** : Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel
- **ETH Zürich**: Prof. Kenneth Paterson, Prof. Srdjan Capkun, Prof. David Basin, Dr. Dennis Jackson, Dr. Jan Beutel
- **KU Leuven**: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Dave Singelée, Dr. Aysajan Abidin
- **TU Delft**: Prof. Seda Guerses
- **University College London**: Dr. Michael Veale
- **CISPA**: Prof. Cas Cremers
- **University of Oxford**: Dr. Reuben Binns
- **University of Torino / ISI Foundation**: Prof. Ciro Cattuto

Contact: dp3t@groupe.epfl.ch