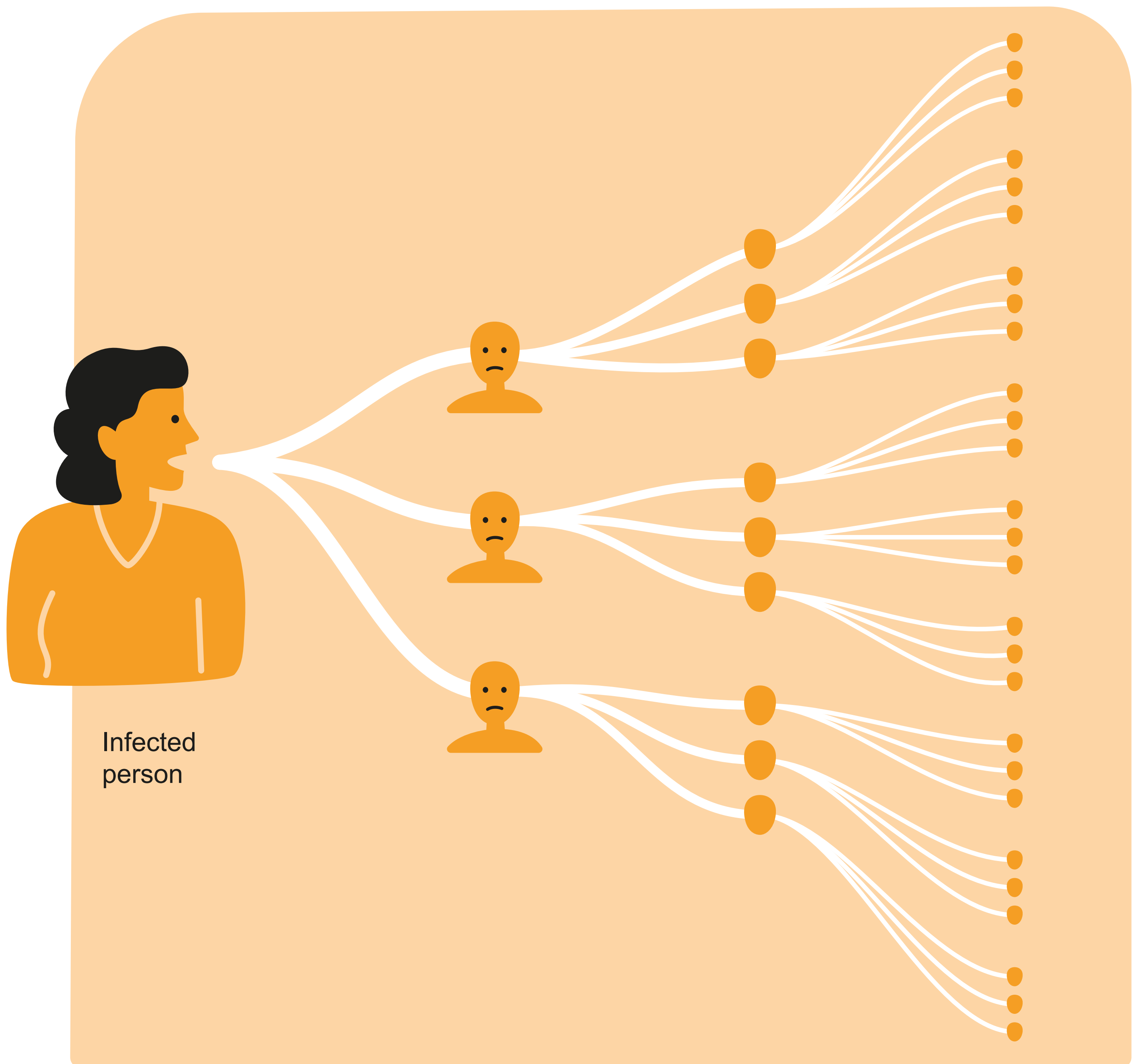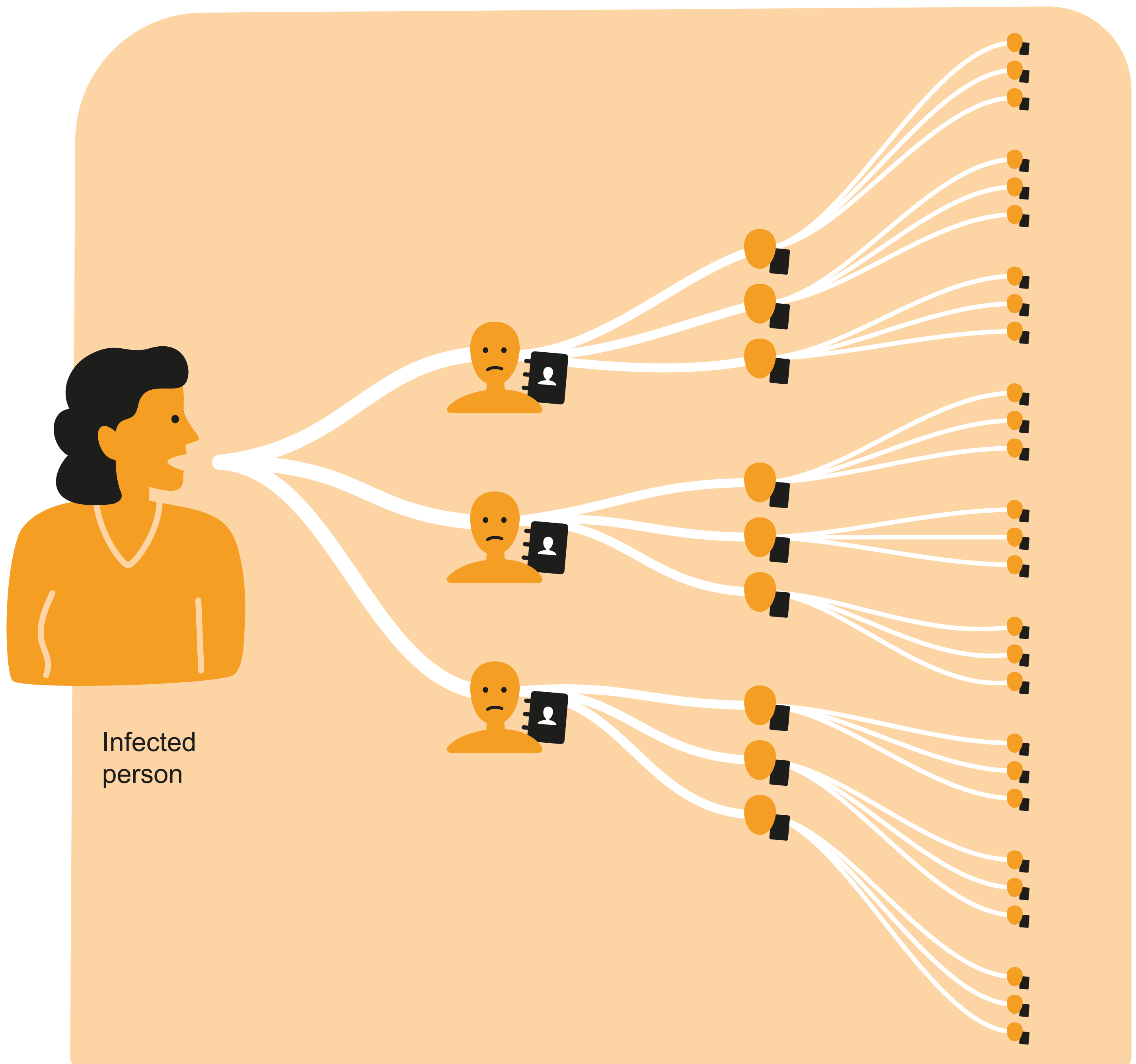# ROBust and privacy-presERving proximity Tracing
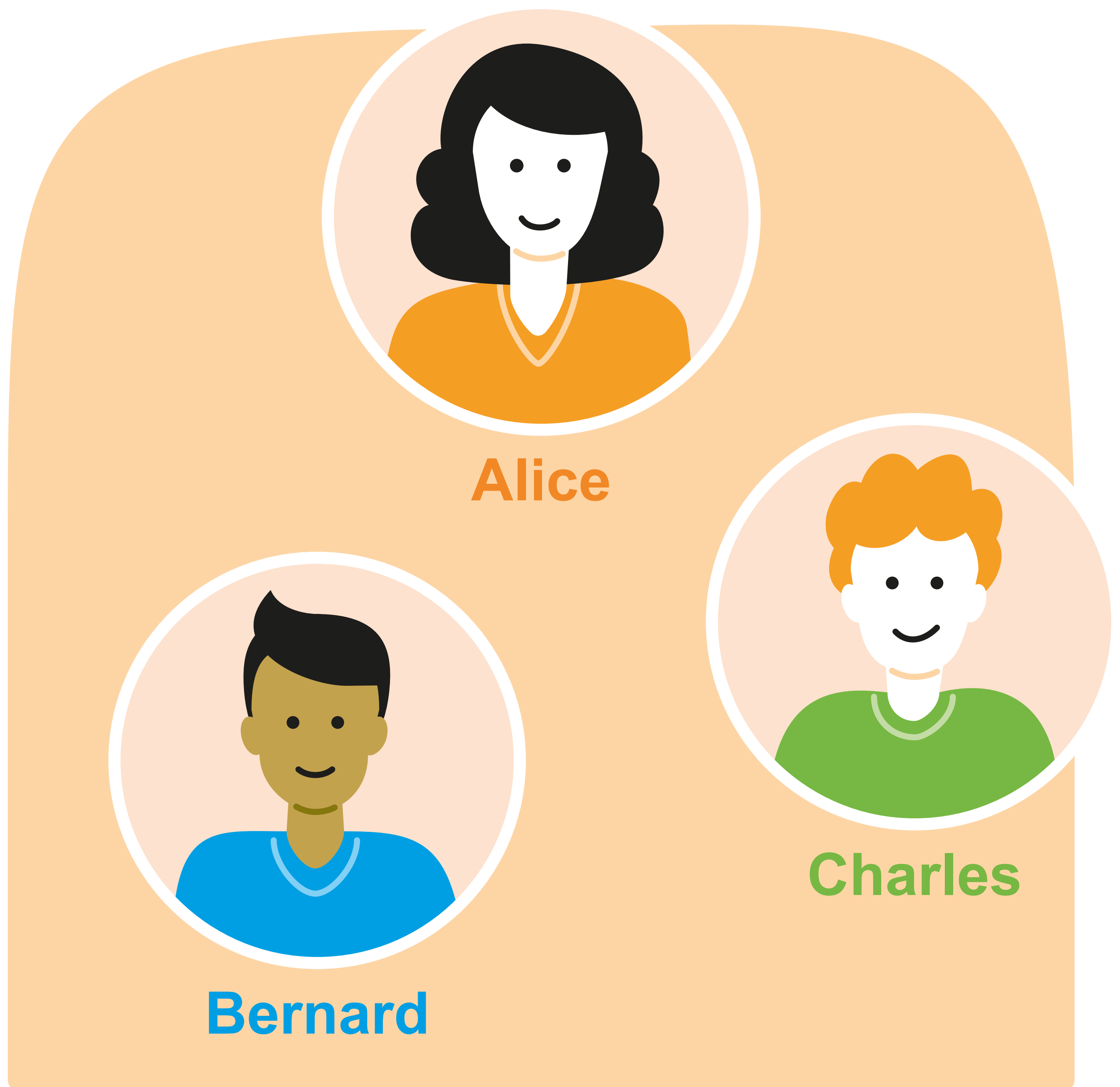
## (ROBERT)

Why is COVID-19 spreading so fast? It's because anybody can be contagious for several days without knowing and without having any symptoms. Such people can transmit the virus to the people around them.

Infected person

In several countries, contacts of infected people have been analysed manually by health authority workers by collecting personal data of infected people or using their geolocation.

**ROBERT Protocol**

It is possible to trace proximity of infected people with a smartphone application in a privacy-preserving manner, simply relying on Bluetooth signals. We propose that such an application is implemented using the ROBERT Protocol.

**ROBERT Protocol**

How can an application trace infected users and protect their privacy? Follow the story of three people, Alice, Bernard, and Charles, to see how the ROBERT Protocol works.

Alice decides to install an application and activates Bluetooth. This is an application that is based on the ROBERT protocol.

Upon installation, an application receives several pseudonyms. Those pseudonyms will be used one after the other and for a limited period to ensure that they cannot be used to track Alice.

ROBERT Protocol

Application of Alice distributes her pseudonyms via Bluetooth. Only applications of people around Alice, such as Bernard and Charles, are able to capture her pseudonym and store it on their phones.
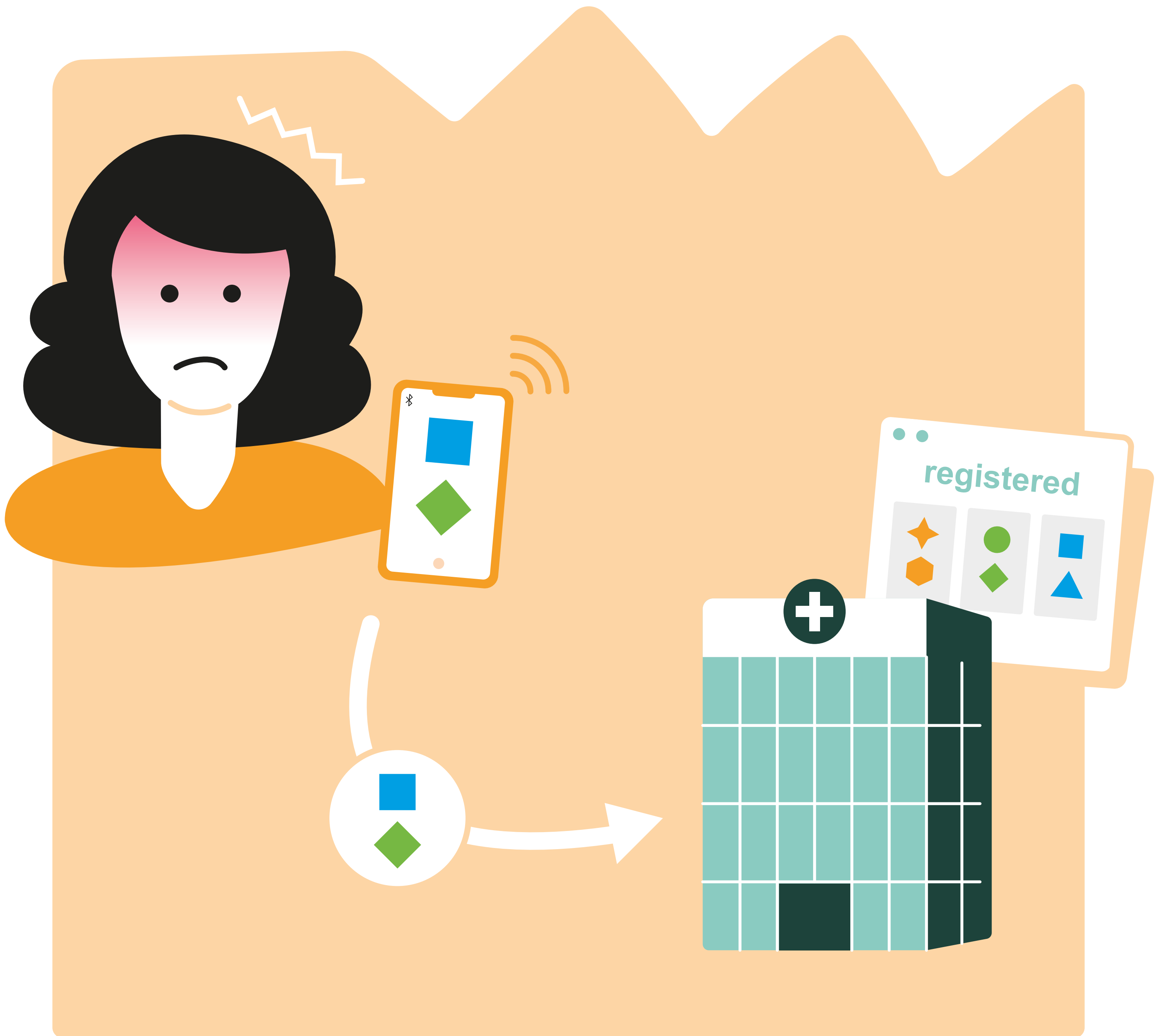
ROBERT Protocol

All the pseudonyms of users around Alice are detected without any information about geolocation. Thanks to the usage of only Bluetooth signals, no one knows where exactly Alice has been.

ROBERT Protocol

A few days later, Alice has COVID-19 symptoms and gets tested. Turns out, Alice has been infected for quite some time now.

To help people who have been around Alice in the last 2 weeks, she agrees to share their pseudonyms with the central database.

ROBERT Protocol

Charles's application sends his pseudonym to the central database several times per day. Charles receives an alert on his smartphone: in the last 2 weeks he has been close to someone infected with COVID-19! Bernard receives the same alert on his smartphone.

ROBERT Protocol

## CAN ANYBODY SPY ON ME BECAUSE I INSTALLED THE APPLICATION BASED ON THE ROBERT PROTOCOL?



No. Let's take Alice for example: upon installation of an application, the central database sends several pseudonyms that get associated with Alice's application. But the central database does not know that it's Alice — it doesn't have any access to her real name, phone number or her location.

**FAQs**

# THAT'S VERY NICE BUT... CAN CHARLES KNOW THAT IT WAS ALICE WHO COULD HAVE PASSED THE VIRUS TO HIM?



No, Charles cannot learn with certainty that it was Alice who became infected. Charles met several people during the day, including Alice and Bernard. When Charles receives an alert if he met only a few people, he could guess who could have passed the virus to him. Researchers are working now on a new version of the ROBERT protocol to protect infected users from such guesses.

# CAN ANYBODY ELSE THAN ALICE'S DOCTOR LEARN THAT ALICE GOT INFECTED?
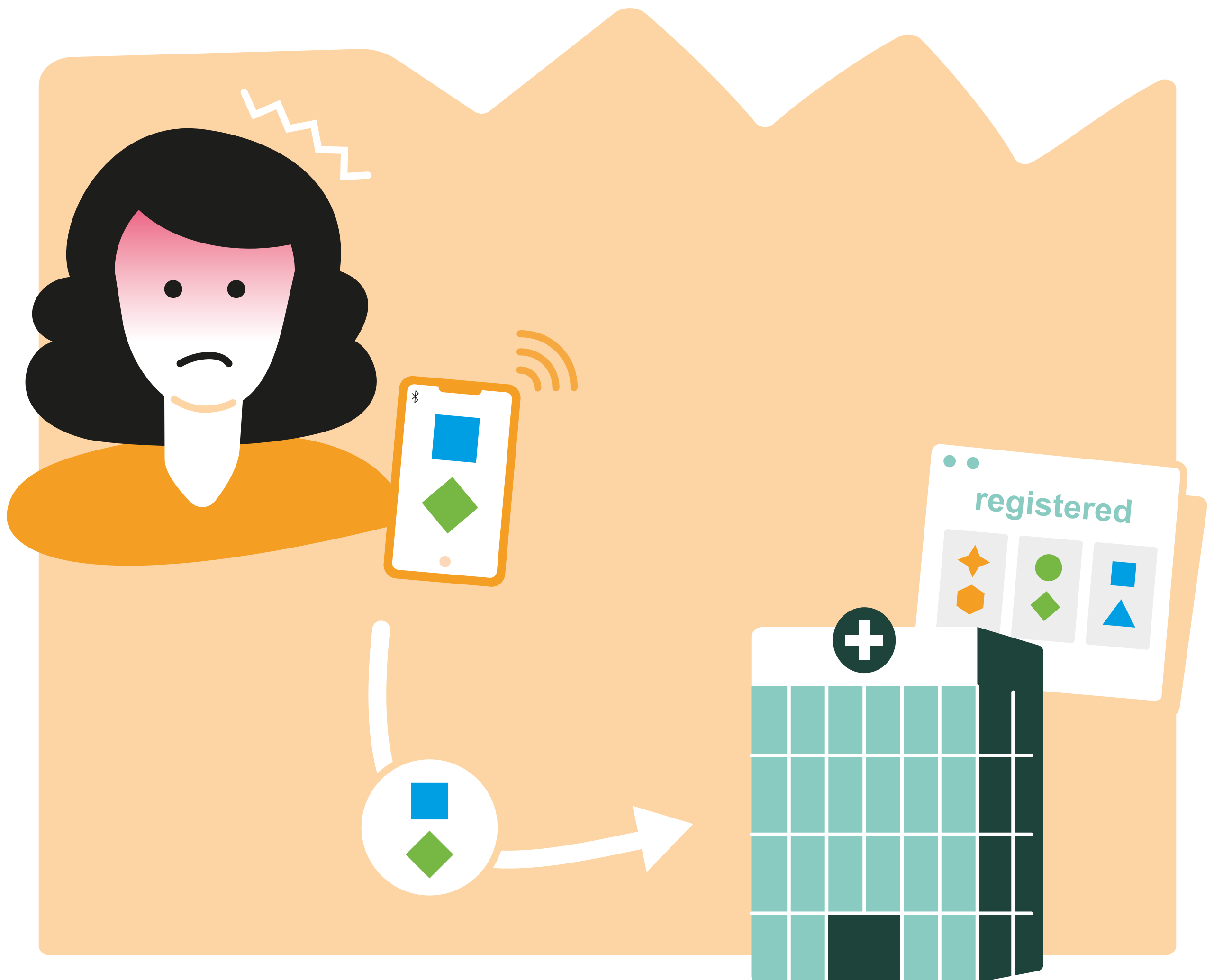


No. The ROBERT Protocol ensures that nobody except for the doctor has access to the medical secret of infected users. Even the central database does not get any information on who was infected. The central database only receives temporary pseudonyms of all people who have been close to someone infected. In our example, the central database only receives pseudonyms of Bernard and Charles, but has no information about Alice.

## WHAT ABOUT ELISA, ALICE'S DAUGHTER, WHO DOES NOT HAVE A SMARTPHONE?



Indeed, children and other people who do not have smartphones cannot benefit from such an application. Researchers today are working to ensure that the ROBERT Protocol can operate on a different device that provides the same service to people like Elisa.

**ROBERT Protocol**

# IS "ROBERT" A SMARTPHONE APPLICATION?



No, ROBERT is not an application. It's a communication protocol — in informatics this means a "procedure" that describes how an application should work. It's proposed by scientists, who have been working on security and privacy of communication protocols for more than 20 years. Any application can use the ROBERT Protocol. ROBERT is a proposal for a Pan European Privacy-Preserving Proximity Tracing (PEPP-PT) initiative, which main goal is to respect the European standards in data protection, privacy and security.

# ROBERT technical specification:
## https://github.com/ROBERT-proximity-tracing

April 2020