



European-Wide Privacy-Preserving Proximity Tracing

Prof. dr. ir. Bart Preneel

Bart.Preneel(AT)esat.kuleuven.be @cosic.be
@bpreneel1

9 October 2020

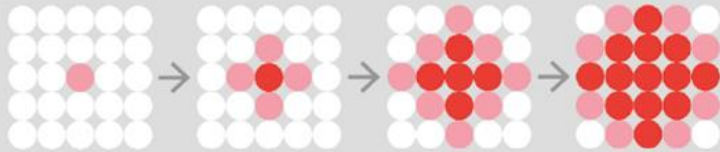


What is contact tracing ?

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

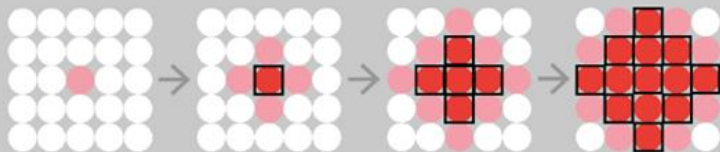


If we do nothing



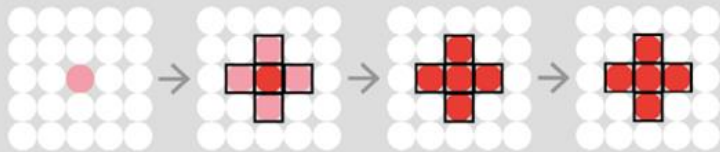
We get a wave of infections

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



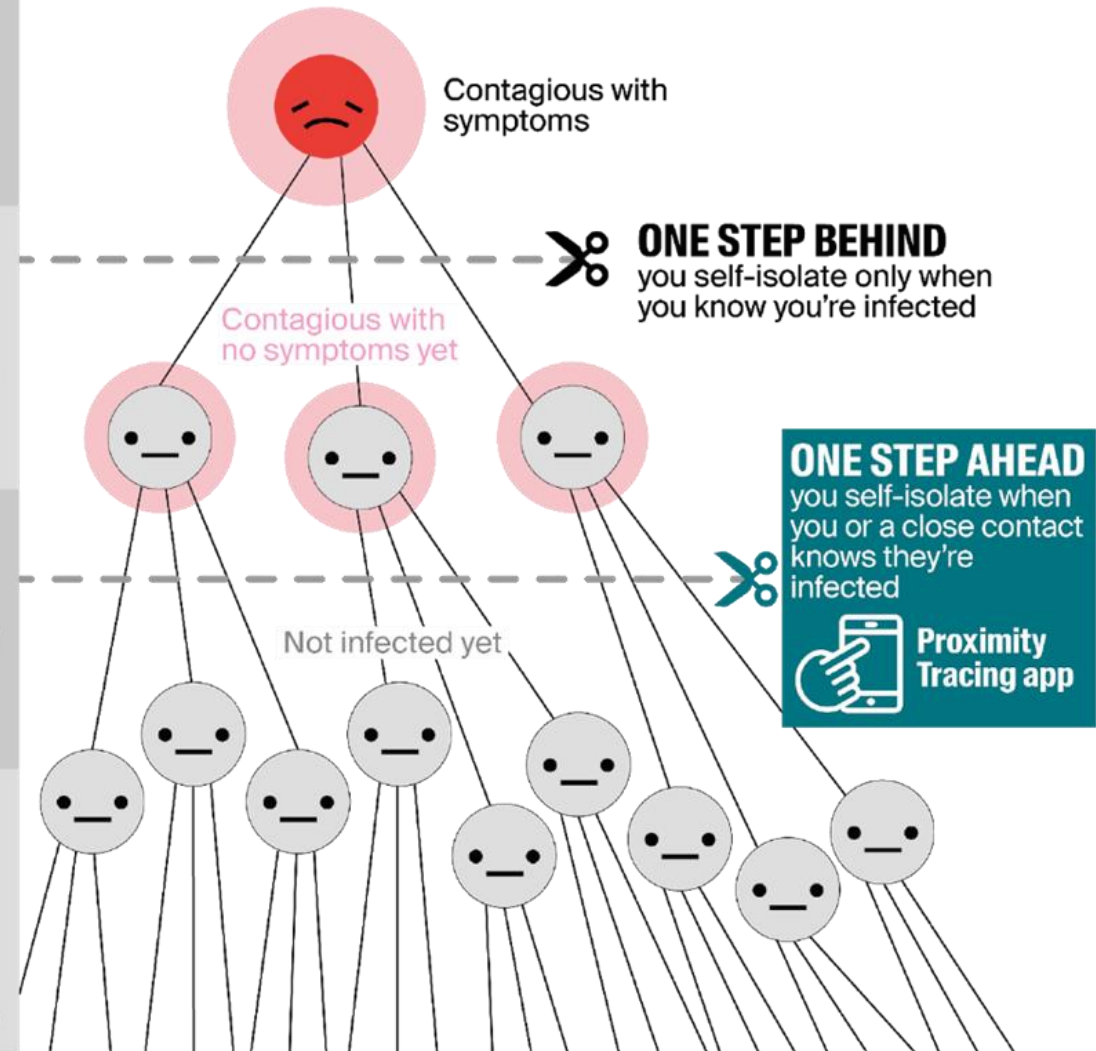
We are one step behind the virus

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



We are one step ahead

Test-Isolate-Quarantine



Contact tracing

= essential to control epidemic

Conditions:



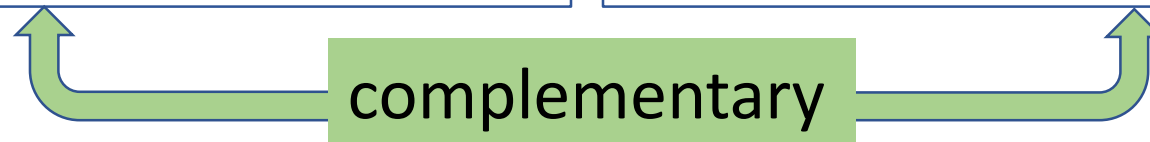
Sufficient testing
Sufficient capacity
Support in society

Manual (contacts)

- Privacy invasive (unavoidable)
- Slow
- Accuracy:
 - human memory
 - what with contacts with strangers?

App (proximity)

- Privacy by design
- Faster
- More accurate
 - false positives/negatives
 - also with strangers



Contact tracing via app: requirements

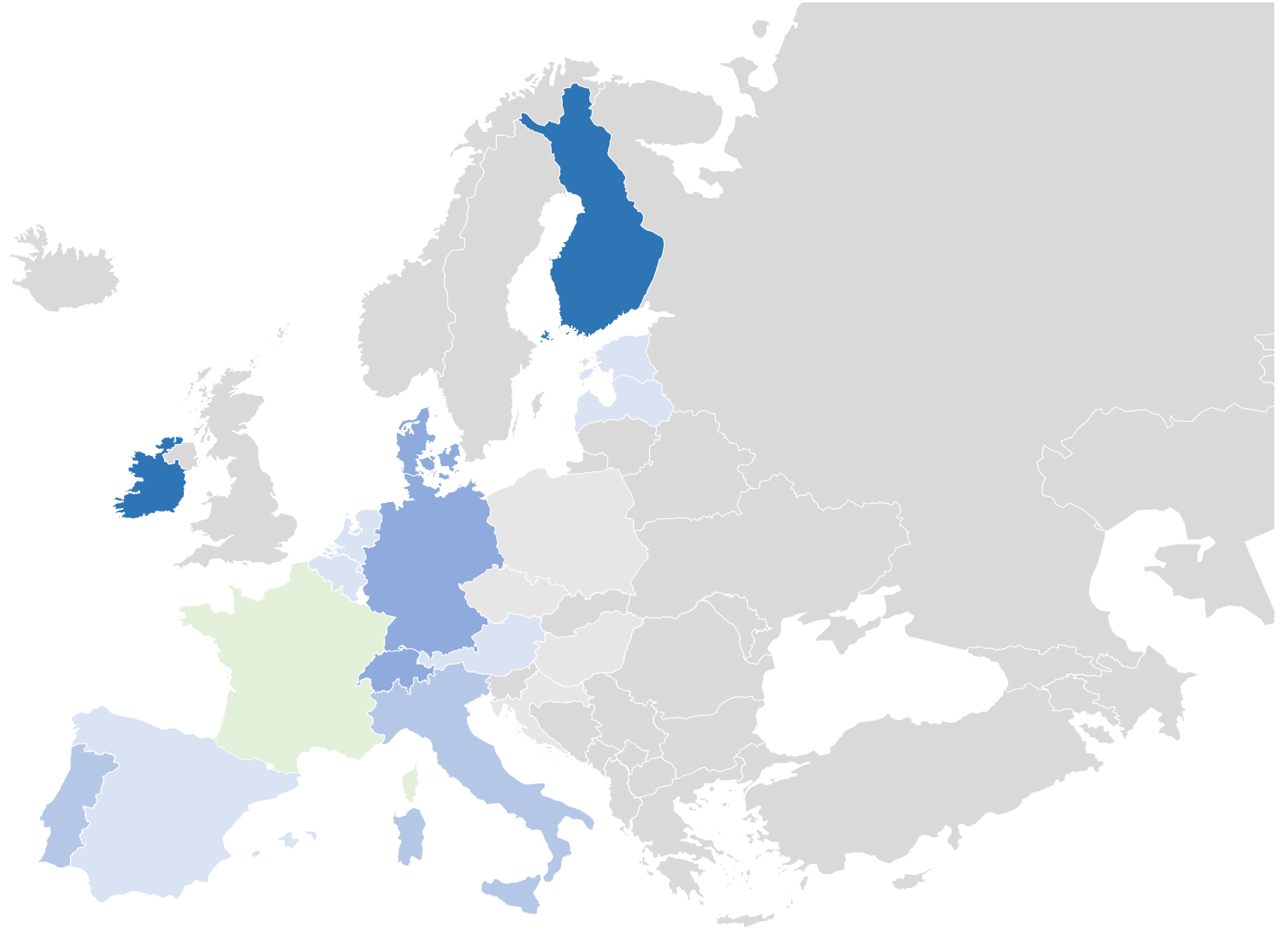
- Accuracy:
 - Only for sufficiently intensive contacts
 - Minimize false negatives and false positives
- Security: avoid false or incorrect reporting of infections (i.e. no self-reporting)
- Scalable to 100+ million users
- Transparency: specs and software open
- Voluntary: needs confidence of the general public
- Fast deployment

DP3T Consortium

- Backed by multidisciplinary research team:
<https://github.com/DP-3T>
- Supported by Google (Android) and Apple (iOS)
- Privacy by design – data minimization: GDPR-compatible
- EU de facto standard - EU interoperability expected by mid October 2020

45 million downloads of DP3T based apps in EU + CH

- 18 EU countries + CH
- Adoption rates from 1-42% (average: 15%)
- France: centralized and not compatible

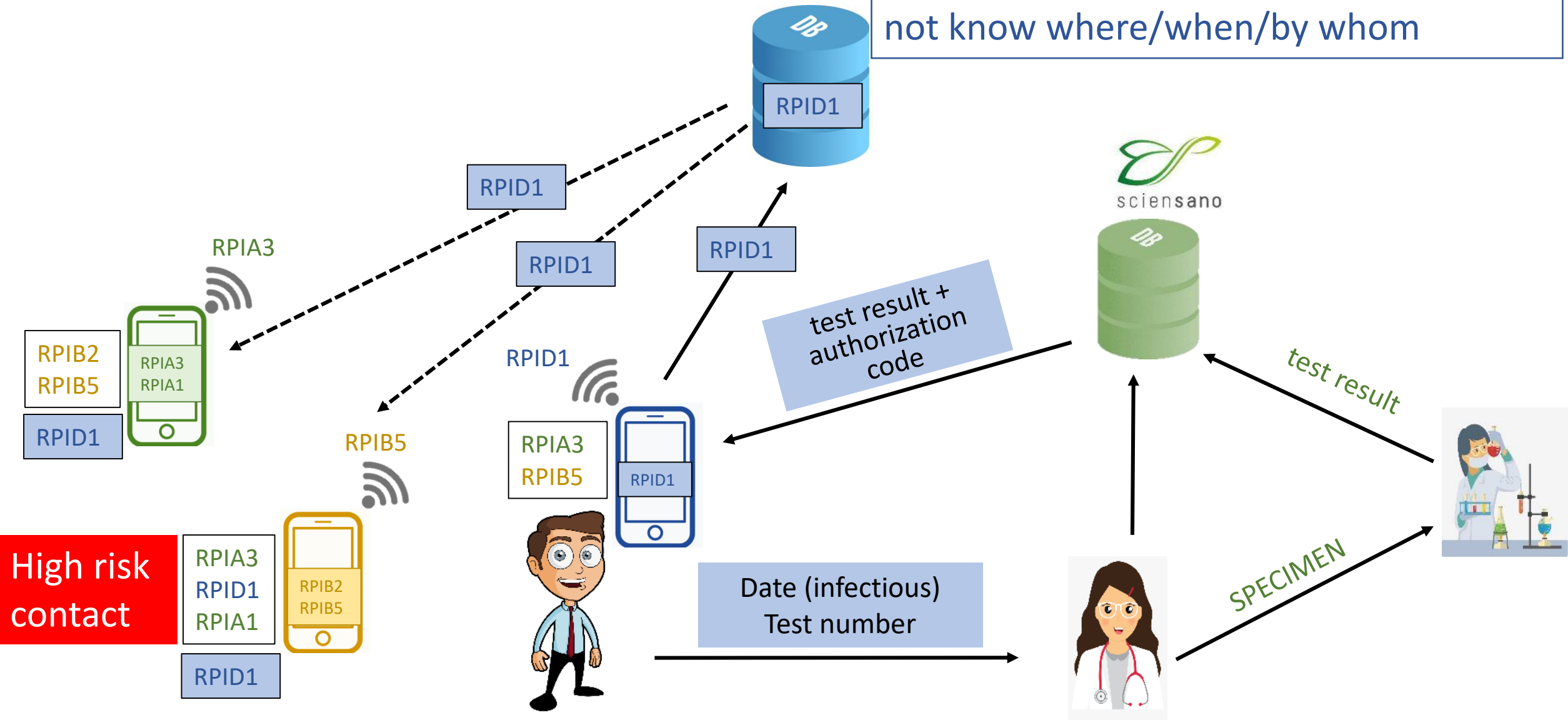


Adoption rate?

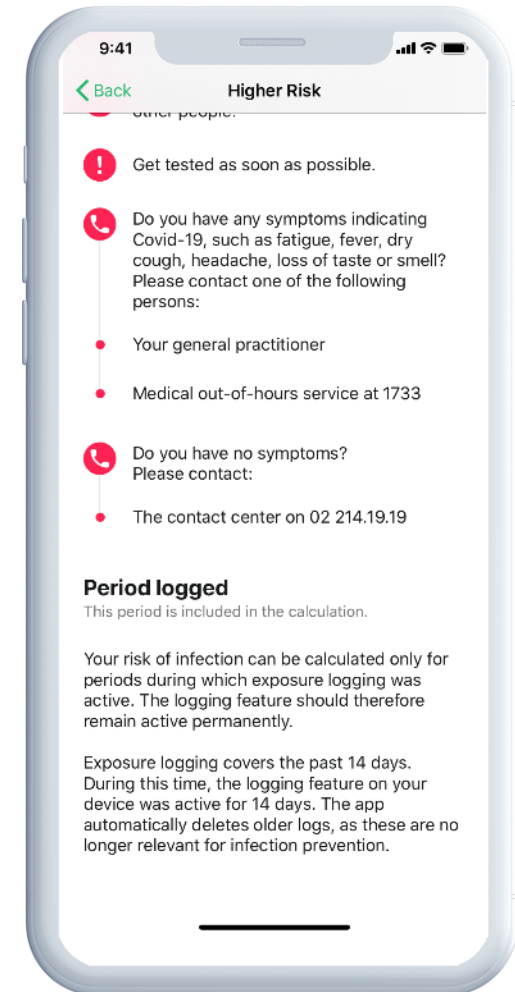
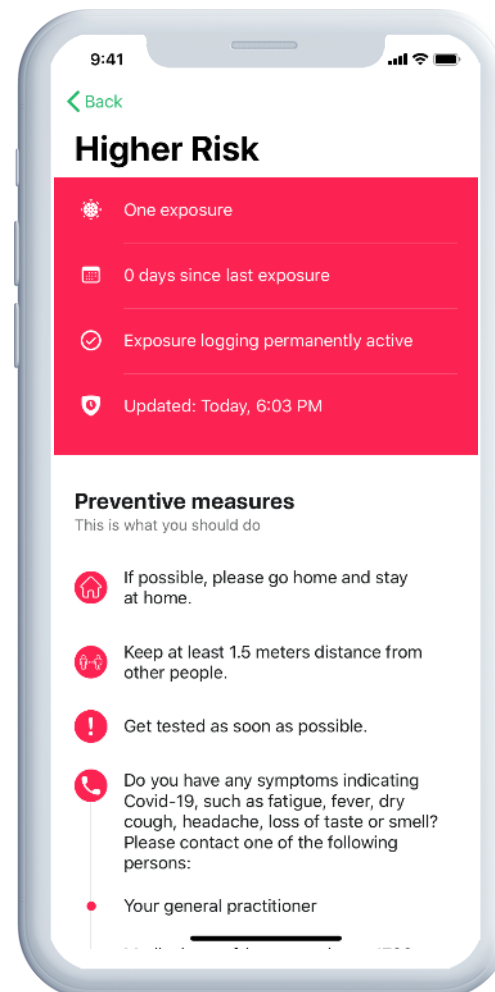
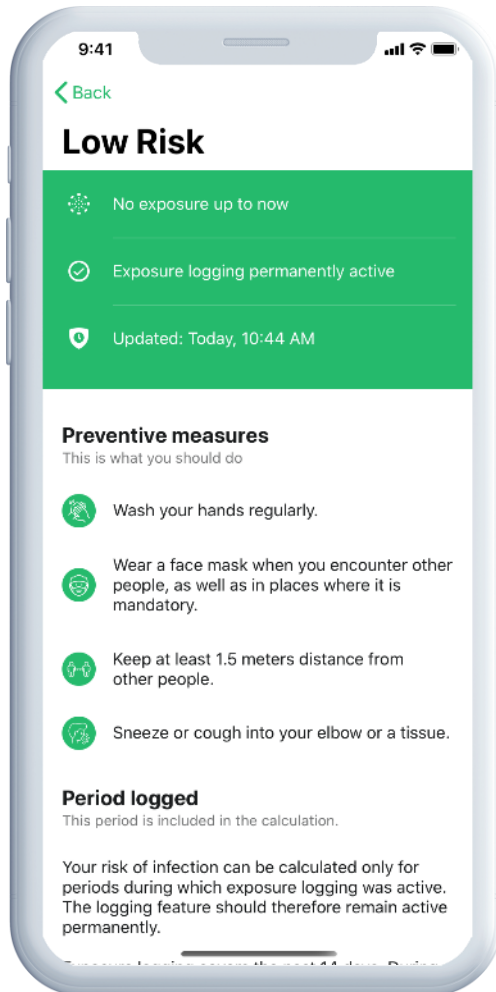
- Misquoted study from Oxford University (April 2020): 60%
 - Assumes no other tracing
- New research (September 2020)
 - Can identify new cases not detected with manual tracing even at low adoption rates
 - Particularly effective in certain groups (work, university) with substantial adoption (30% or higher)

Telephones send/store random Bluetooth signals

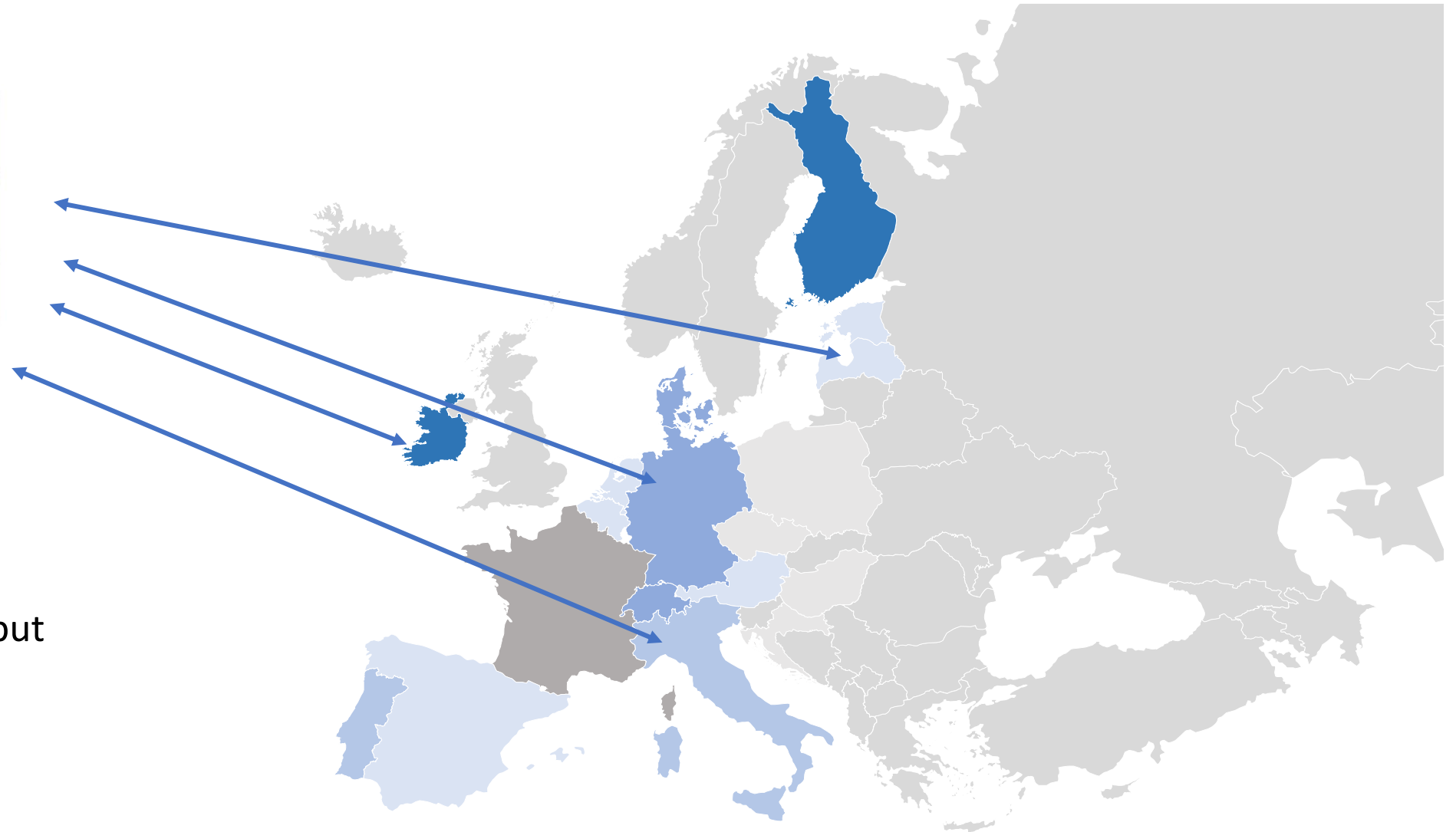
Central database only stores random data (pseudonyms) of infected people
User informed of risk contact but does not know where/when/by whom



Be notified



European Federation Gateway Service (mid October)



Apps not identical but
can interoperate

Bart Preneel, COSIC, at KU Leuven and imec

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: homes.esat.kuleuven.be/~preneel/

EMAIL: Bart.Preneel@esat.kuleuven.be

TWITTER: [@bpreneel1](https://twitter.com/bpreneel1)

TELEPHONE: +32 16 321148



More information on Coronalert

- <https://github.com/DP-3T>
- <https://coronalert.be/>
- Code: <https://github.com/DP-3T/documents>
- Specification: <https://www.corona-tracking.info/wp-content/uploads/2020/08/Coronalert-description-v1.3.pdf>
- Public consultation:
<https://www.esat.kuleuven.be/cosic/sites/corona-app/>