COSIC

KU LEUVEN

imec
embracing a better life

Privacy-friendly proximity and presence tracing

Prof. dr. ir. Bart Preneel

Bart.Preneel(AT)esat.kuleuven.be

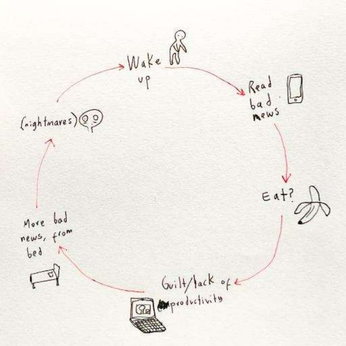
@bpreneel1

Secappdev – 13 June 2022 – v1

Outline

- Big data and corona
- Digital proximity tracing
- Evaluation
- Presence detection

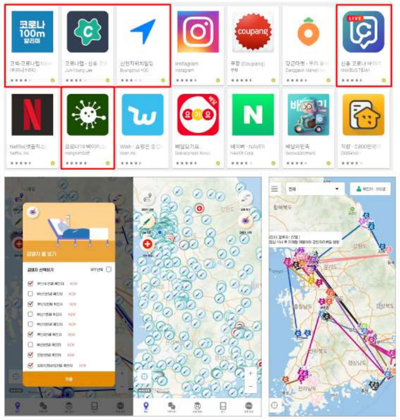
Can technology help us to deal with Corona?



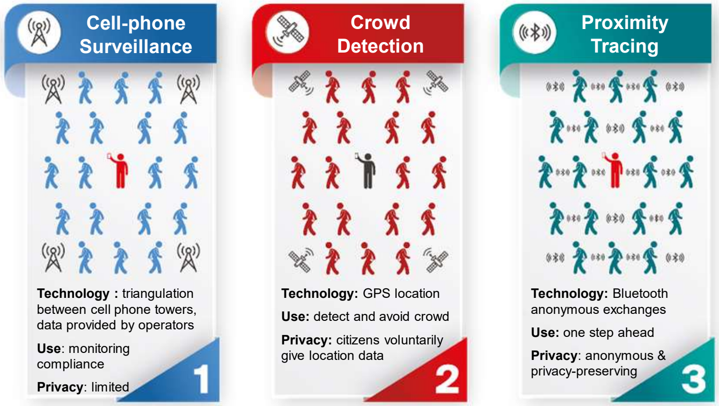
- Information
- Self-diagnosis
- Collect medical data
- Location-based techniques

Feb 27, 2020
South Korea:
5 coronavirus-related apps rank within the top 10 apps in the Google Play Store

China: many apps



Individual location-based techniques



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

Use: monitoring compliance

Privacy: limited

Technology: GPS location

Use: detect and avoid crowd

Privacy: citizens voluntarily give location data

Technology: Bluetooth anonymous exchanges

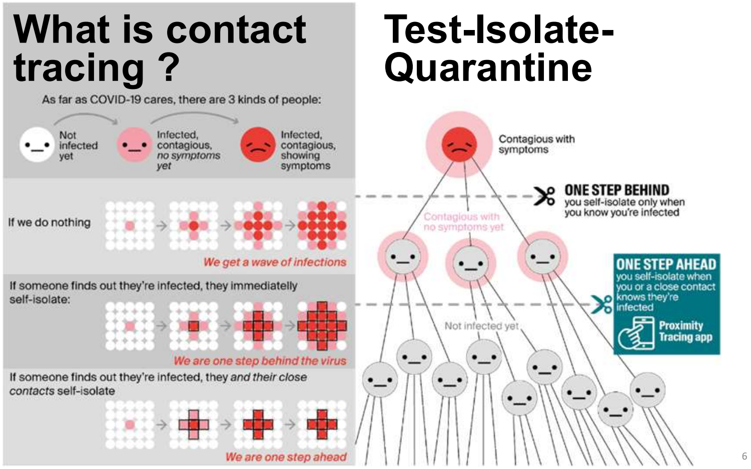
Use: one step ahead

Privacy: anonymous & privacy-preserving

https://www.google.com/covid19/mobility/

What is contact tracing ?

Test-Isolate-Quarantine


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

Not infected yet
Infected, contagious, *no symptoms yet*
Infected, contagious, showing symptoms

If we do nothing

We get a wave of infections

If someone finds out they're infected, they immediatelly 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

Contagious with symptoms
Contagious with no symptoms yet
Not infected yet

ONE STEP BEHIND you self-isolate only when you know you're infected

ONE STEP AHEAD you self-isolate when you or a close contact knows they're infected

Contact tracing
= essential to control epidemic

Conditions:
- Sufficient testing
- Sufficient capacity
- Support in society

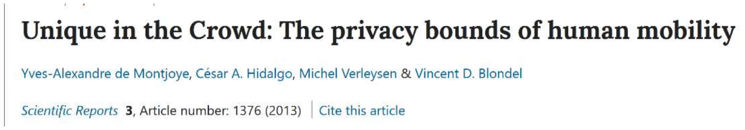
Manual (contacts)
- Privacy invasive (unavoidable)
- Slow & expensive
- Accuracy
  - human memory
  - what with contacts with strangers?

App (proximity)
- Privacy by design
- Faster
- More accurate
  - false positives/negatives
  - also with strangers

complementary

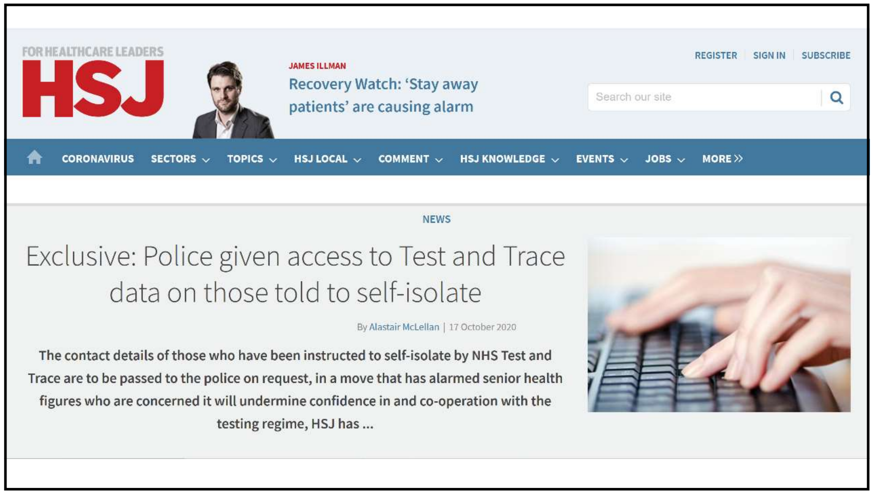
Proximity tracing: geolocation (GPS)

- Examples: South-Korea, Israel (+ Google location data), Norway
- Major privacy problem: 4 space-time points identify 95% of individuals


Unique in the Crowd: The privacy bounds of human mobility

Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel

Scientific Reports **3**, Article number: 1376 (2013) | Cite this article

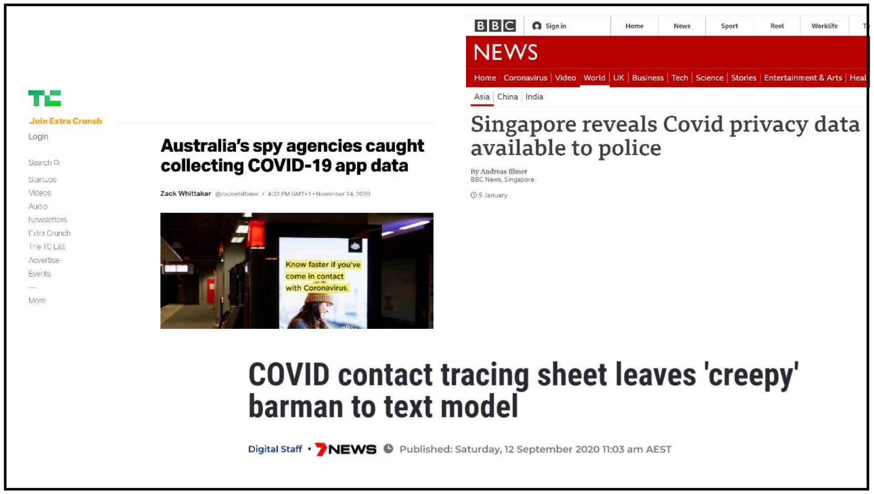


FOR HEALTHCARE LEADERS
HSJ
JAMES ILLMAN
Recovery Watch: 'Stay away patients' are causing alarm
REGISTER SIGN IN SUBSCRIBE
Search our site
CORONAVIRUS SECTORS TOPICS HSJ LOCAL COMMENT HSJ KNOWLEDGE EVENTS JOBS MORE
NEWS

Exclusive: Police given access to Test and Trace data on those told to self-isolate

By Alastair McLellan | 17 October 2020

The contact details of those who have been instructed to self-isolate by NHS Test and Trace are to be passed to the police on request, in a move that has alarmed senior health figures who are concerned it will undermine confidence in and co-operation with the testing regime, HSJ has ...



TC
Join Extra Crunch
Login
Search
Startups
Videos
Audio
Newsletters
Extra Crunch
The TC List
Advertise
Events
More
Know faster if you've come in contact with Coronavirus.
BBC
Sign in
Home
News
Sport
Reel
Worklife
NEWS
Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Heal
Asia | China | India

Australia's spy agencies caught collecting COVID-19 app data

Zack Whittaker @zackwhittaker / 4:32 PM GMT+1 • November 24, 2020

Singapore reveals Covid privacy data available to police

By Andreas Illmer
BBC News, Singapore

5 January

COVID contact tracing sheet leaves 'creepy' barman to text model

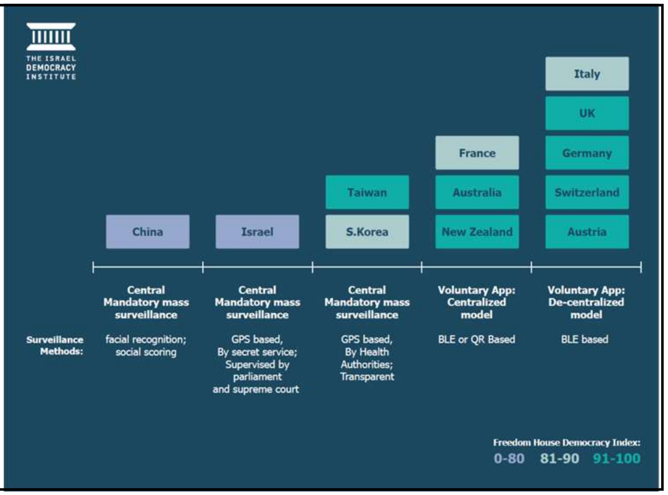
Digital Staff • 7NEWS Published: Saturday, 12 September 2020 11:03 am AEST

Norway pulls its coronavirus contacts-tracing app after privacy watchdog's warning

Natasha Lomas @riptari / 5:02 PM GMT+2 • June 15, 2020

Image Credits: elenabs / Getty Images

Status: July 2020



THE ISRAEL DEMOCRACY INSTITUTE
Italy
UK
Germany
Switzerland
Austria
France
Australia
New Zealand
Taiwan
S.Korea
China
Israel
Central Mandatory mass surveillance
Central Mandatory mass surveillance
Central Mandatory mass surveillance
Voluntary App: Centralized model
Voluntary App: De-centralized model
Surveillance Methods:
facial recognition; social scoring
GPS based, By secret service; Supervised by parliament and supreme court
GPS based, By Health Authorities; Transparent
BLE or QR Based
BLE based
Freedom House Democracy Index:
0-80
81-90
91-100

Decentralized Proximity tracing: requirements (1/2): Respect for privacy and human rights

- Data minimization – privacy by design (GDPR)
  - No central database that can reconstruct social graph/count
- Data can only be used to detect proximity
  - Built-in protection against "function creep"
- Protect identities: who has been in contact with whom, where and when
  - No information about uninfected users
- Right to be forgotten (erase data): auto-fading

Decentralized Proximity tracing: requirements (2/2)

- 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

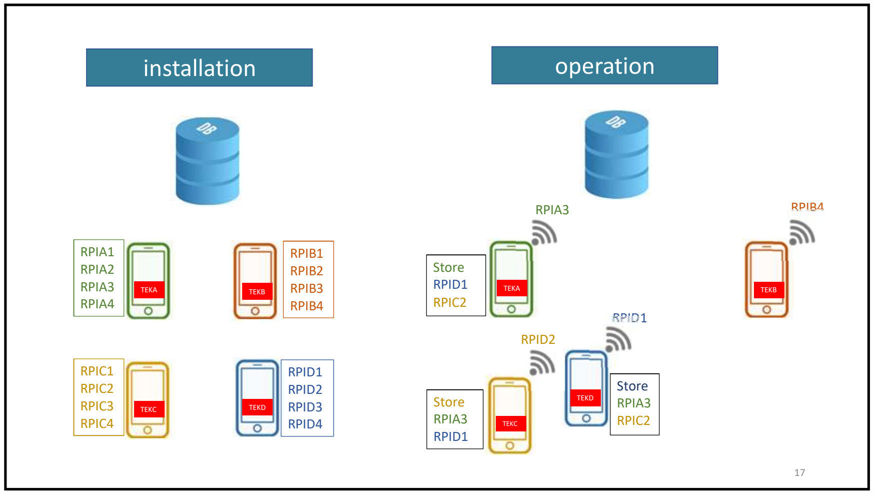
Realistic deployment: Google/Apple Exposure API

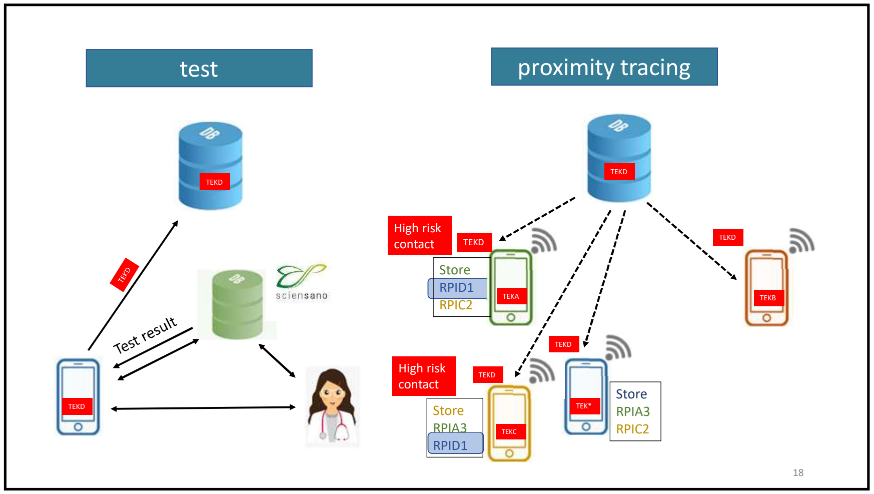
- Android and iOS versions need to be compatible
- Battery and CPU usage
  - No connections/limited roundtrips
- Run in background: need iOS/still problems on some Android phones
- Support for old(er) devices
- Google and Apple implement protocol and API
  - privacy engineering
  - epidemiology and exposure estimation
  - internationalization
  - deployment
- Fall 2020: Apple iOS 13.7 – Exposure Notification Express

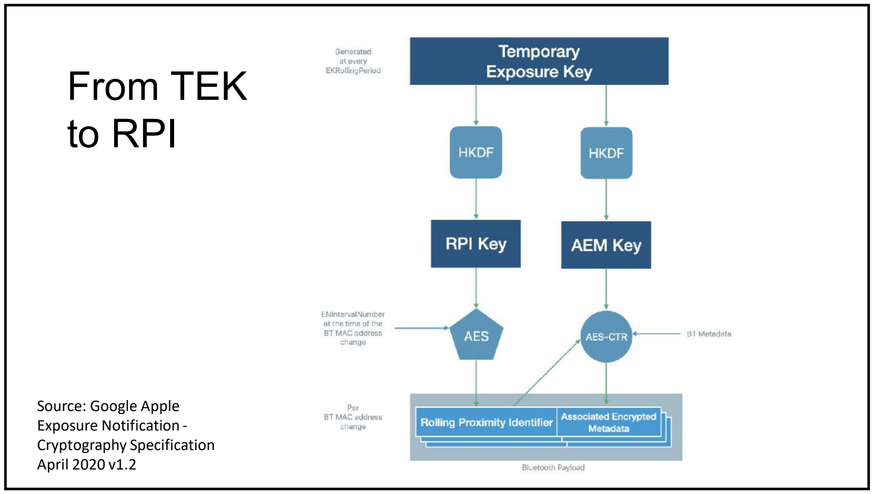
DP3T Protocol History

- March 2020: multidisciplinary research team: https://github.com/DP-3T
- March 2020: US PACT East Coast and West Coast
- April 2020: Google (Android) and Apple (iOS) GAEN
- May 2020: protocol and code finished
- June 2020: apps launch in CH/DE & start of EU interoperability (EFGS)
- October 2020: EU server launches

- Asia/Oceania: Japan, Kazachstan, New Zealand, Saudi Arabia
- Russia
- South Africa
- Canada + US: 26 states/territories
- South America: Brazil, Ecuador, Panama, Uruguay
- https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/



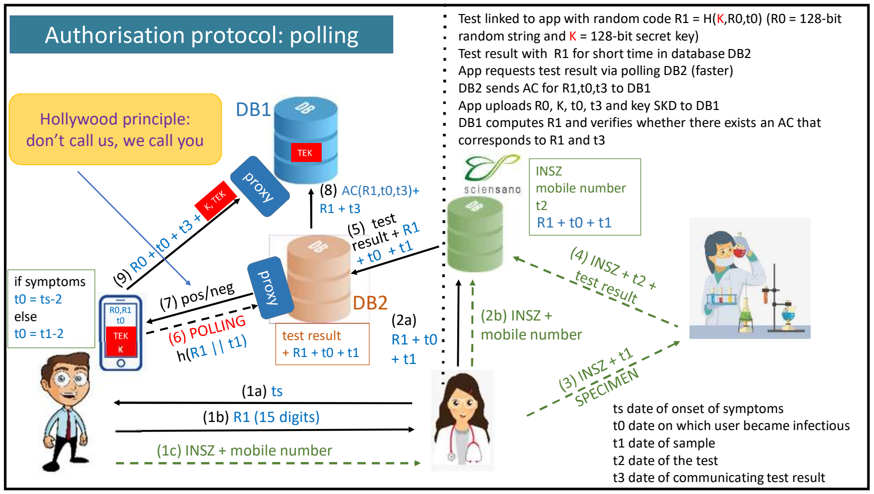




From TEK to RPI

Generated at every EKRollingPeriod
Temporary Exposure Key
HKDF
HKDF
RPI Key
AEM Key
ENIntervalNumber at the time of the BT MAC address change
AES
AES-CTR
BT Metadata
Per BT MAC address change
Rolling Proximity Identifier
Associated Encrypted Metadata
Bluetooth Payload

Source: Google Apple Exposure Notification - Cryptography Specification April 2020 v1.2



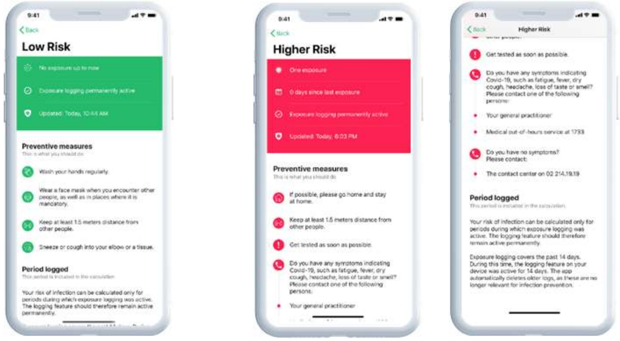
Authorisation protocol: polling

- Test linked to app with random code R1 = H(K,R0,t0) (R0 = 128-bit random string and K = 128-bit secret key)
- Test result with R1 for short time in database DB2
- App requests test result via polling DB2 (faster)
- DB2 sends AC for R1,t0,t3 to DB1
- App uploads R0, K, t0, t3 and key SKD to DB1
- DB1 computes R1 and verifies whether there exists an AC that corresponds to R1 and t3

Hollywood principle: don't call us, we call you
DB1
DB
TEK
proxy
(8) AC(R1,t0,t3)+ R1 + t3
(5) test result + R1 + t0 + t1
(9) R0 + t0 + t3 + K, TEK
if symptoms
t0 = ts-2
else
t0 = t1-2
(7) pos/neg
(6) POLLING h(R1 || t1)
R0,R1 t0
TEK
K
proxy
DB
DB2
test result + R1 + t0 + t1
(2a) R1 + t0 + t1
sciensano
DB
INSZ
mobile number
t2
R1 + t0 + t1
(4) INSZ + t2 + test result
(2b) INSZ + mobile number
(3) INSZ + t1 SPECIMEN
(1a) ts
(1b) R1 (15 digits)
(1c) INSZ + mobile number

ts date of onset of symptoms
t0 date on which user became infectious
t1 date of sample
t2 date of the test
t3 date of communicating test result

Be notified



9:41

Back

Low Risk

No exposure up to now

Exposure logging permanently active

Updated: Today, 10:44 AM

Preventive measures

This is what you should do

Wash your hands regularly.

Wear a face mask when you encounter other people, as well as in places where it is mandatory.

Keep at least 1.5 meters distance from other people.

Sneeze or cough into your elbow or a tissue.

Period logged

This period is included in the calculation

Your risk of infection can be calculated only for periods during which exposure logging was active. The logging feature should therefore remain active permanently.

9:41

Back

Higher Risk

One exposure

0 days since last exposure

Exposure logging permanently active

Updated: Today, 6:03 PM

Preventive measures

This is what you should do

If possible, please go home and stay at home.

Keep at least 1.5 meters distance from other people.

Get tested as soon as possible.

Do you have any symptoms indicating Covid-19, such as fatigue, fever, dry cough, headache, loss of taste or smell? Please contact one of the following persons:

- Your general practitioner

9:41

Back Higher Risk

Get tested as soon as possible.

Do you have any symptoms indicating Covid-19, such as fatigue, fever, dry cough, headache, loss of taste or smell? Please contact one of the following persons:

- Your general practitioner
- Medical out-of-hours service at 1733

Do you have no symptoms? Please contact:

- The contact center on 02 214.19.19

Period logged

This period is included in the calculation

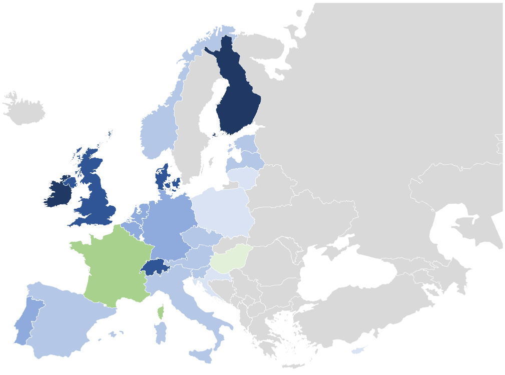
Your risk of infection can be calculated only for periods during which exposure logging was active. The logging feature should therefore remain active permanently.

Exposure logging covers the past 14 days. During this time, the logging feature on your device was active for 14 days. The app automatically deletes older logs, as these are no longer relevant for infection prevention.

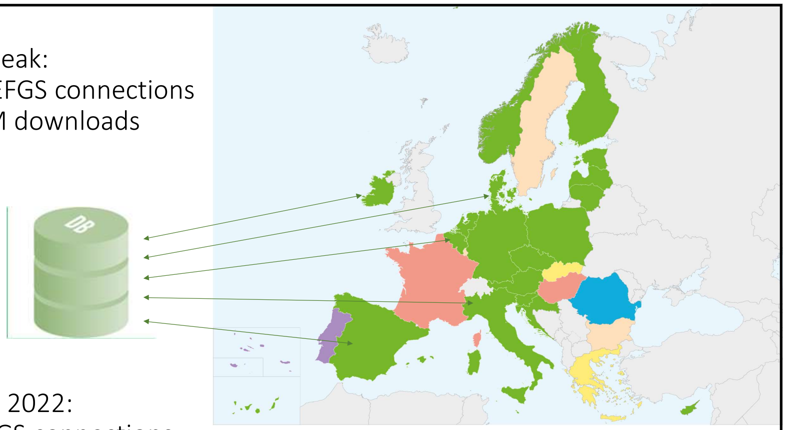
100+ million downloads of DP3T-based apps in EU + CH + Norway + UK

Download rates per country

- HR, CY, PL, LT: 3-11%
- CZ, ES, AT, IT, LV, SI, MT, NO, EE: 15-24%
- BE, NL, DE, PT: 31-35%
- DK, CH, UK: 36-45%
- IE: 50%
- FI: 56%
- [FR: 67%]



@ peak:
19 EFGS connections
73M downloads

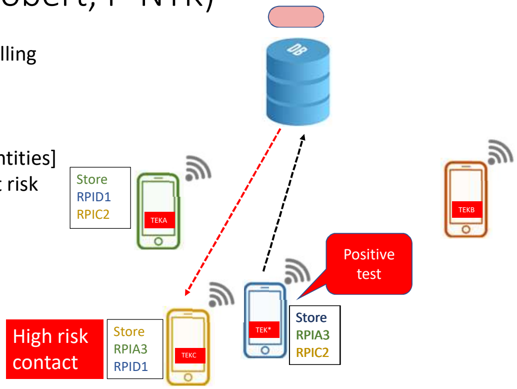


June 2022:
9 EFGS connections

- 🟩 Countries registered with the interoperability gateway service
- 🟪 Countries with a decentralised mobile contact tracing app
- 🟥 Countries with a centralised mobile contact tracing app
- 🟨 Countries with contact tracing app under development
- 🟦 Countries with contact tracing app being planned
- 🟧 Countries with no contact tracing app foreseen

Centralized Proximity Tracing (Singapore, Robert, P-NTK)

Infected person uploads received Rolling Proximity Identifiers (RPIs)
All users upload sent RPIs every day
[Singapore: central authority knows mapping between RPIs and user identities]
Central authority can inform users at risk



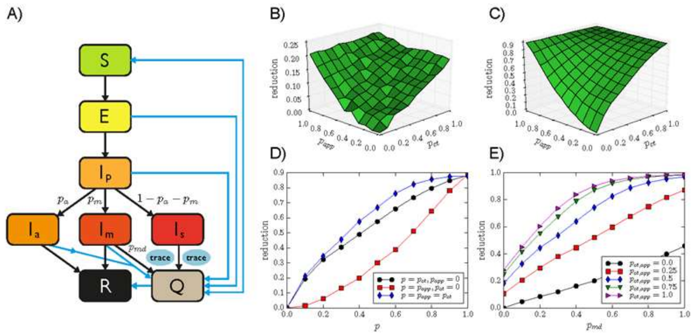
Outline

- Big data and corona
- Digital proximity tracing
- Evaluation
- Presence detection

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)
- Speed matters

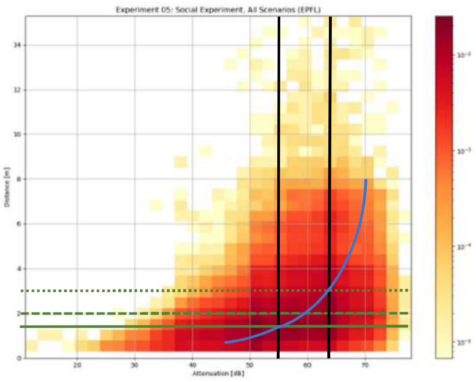
Effectiveness: manual + digital



Barrat et al., Effect of Manual and Digital Contact Tracing on COVID-19 Outbreaks: A Study on Empirical Contact Data, Preprint, July 2020, https://www.medrxiv.org/content/10.1101/2020.07.24.20159947v1

exposure definition: 15 mins
p_{md}= 0.5 probability of mild symptoms

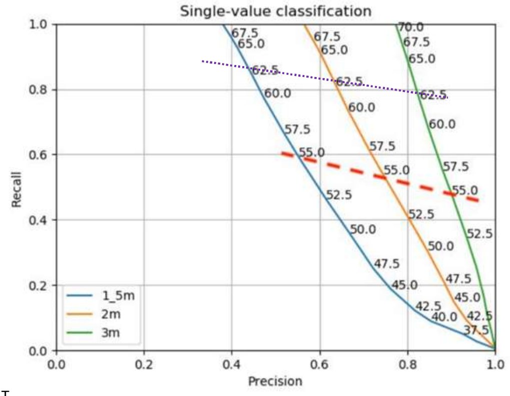
Accuracy: Distance vs. attenuation



Attenuation increases through objects and reflections

Source: DP-3T

Precision and recall



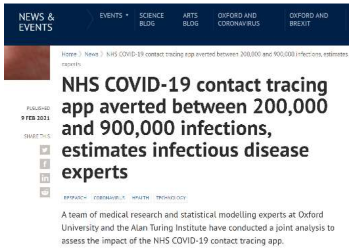
Source: DP-3T

Recall: fraction of beacons from phones within that distance that have attenuation equal or smaller than the threshold (false negatives)

Precision: fraction of beacons for which an attenuation threshold correctly identifies that the phone is within a given distance

England + Wales NHS COVID-19

https://www.ox.ac.uk/news/2021-02-09-nhs-covid-19-contact-tracing-app-averted-between-200000-and-900000-infections



NEWS & EVENTS

EVENTS • SCIENCE BLOG ARTS BLOG OXFORD AND CORONAVIRUS OXFORD AND BREXIT

Home 〉 News 〉 NHS COVID-19 contact tracing app averted between 200,000 and 900,000 infections, estimates experts

PUBLISHED 9 FEB 2021

SHARE THIS

NHS COVID-19 contact tracing app averted between 200,000 and 900,000 infections, estimates infectious disease experts

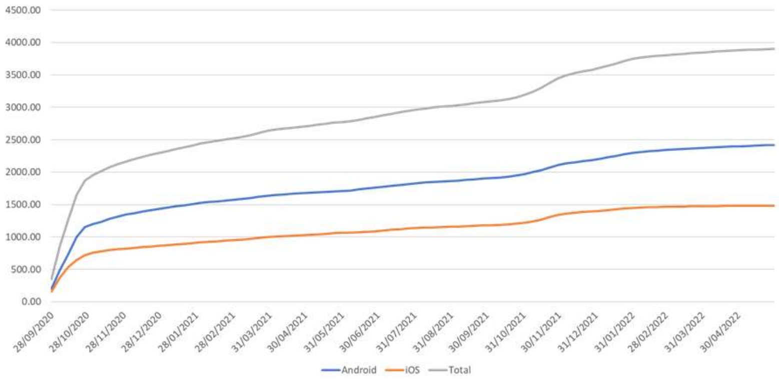
RESEARCH CORONAVIRUS HEALTH TECHNOLOGY

A team of medical research and statistical modelling experts at Oxford University and the Alan Turing Institute have conducted a joint analysis to assess the impact of the NHS COVID-19 contact tracing app.

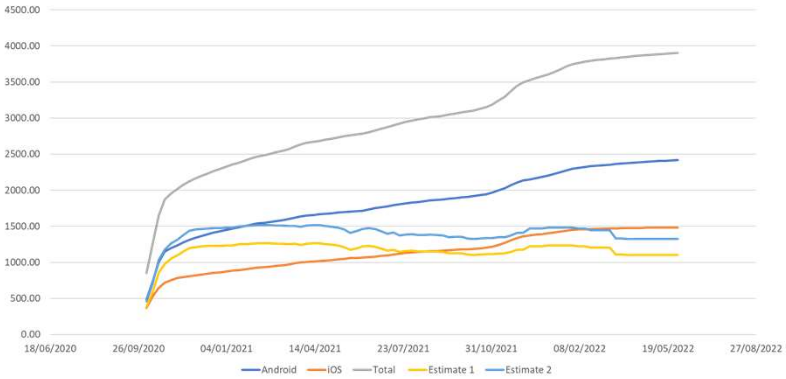
- October-December 2020
- 21 million downloads
- 1.5 million notifications
- For each 1% increase in users we estimate the number of cases will drop by between 0.8% and 2.3%
- 4.4 quarantine notifications per index case

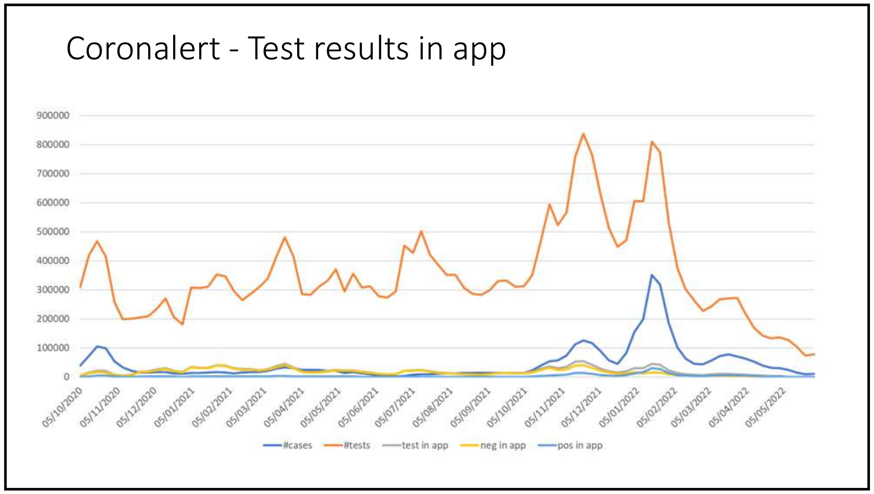
Evaluation is tricky: J. Benzler, D. Bogdanov, G. Kirchner, W. Lueks, R. Lucas, R. Oliveira, B. Preneel, M. Salathe, C. Troncoso, V. von Wyl, Towards a common performance and effectiveness terminology for digital proximity tracing applications. https://arxiv.org/abs/2012.12927

Coronalert: Downloads

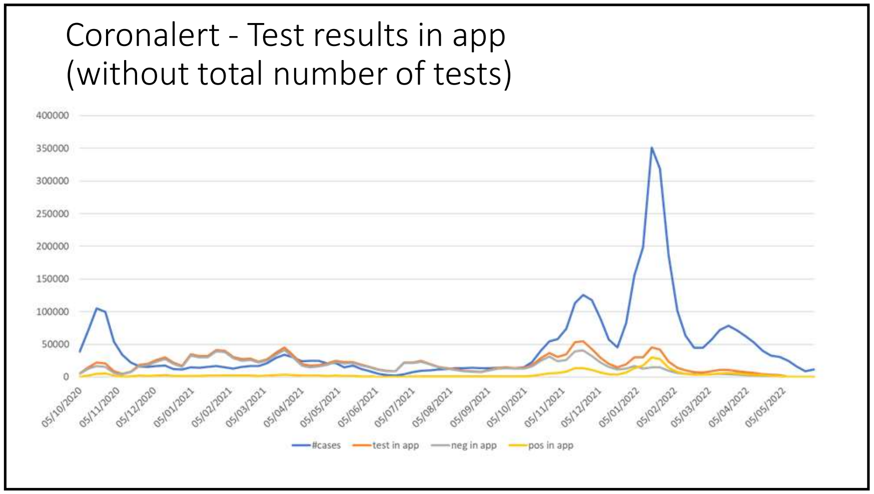


Coronalert: Downloads and Estimates for Active Users

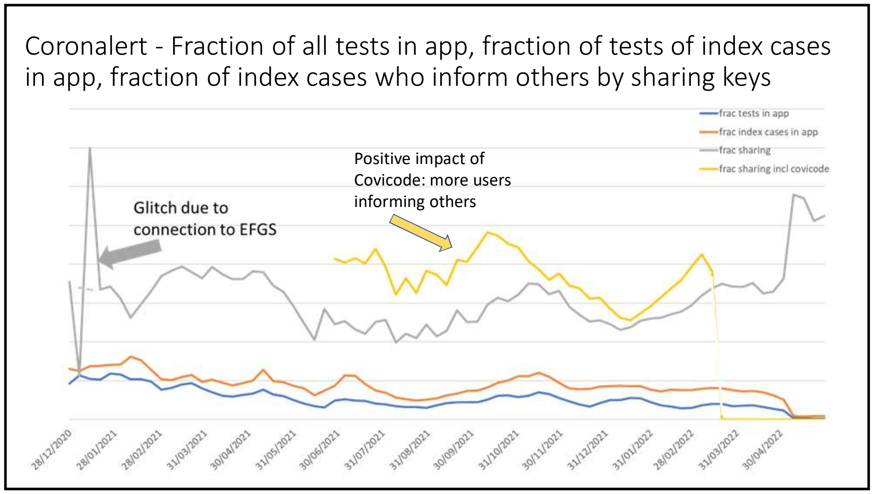




Coronalert - Test results in app



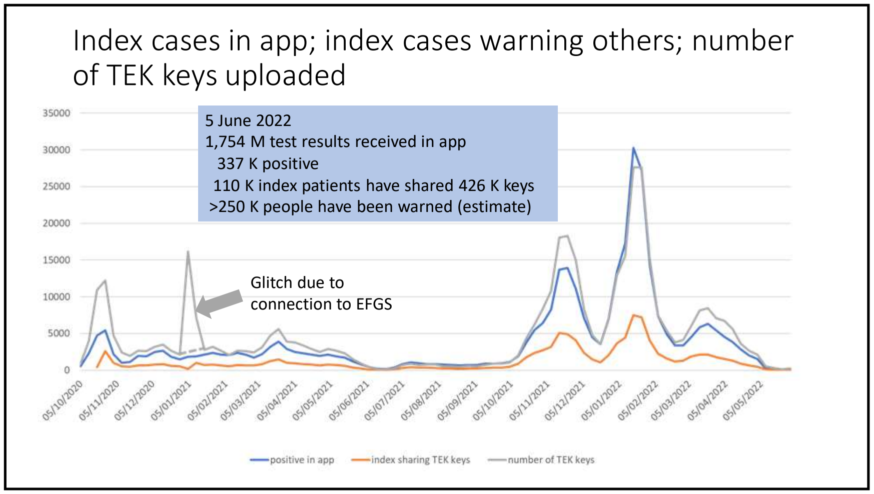
Coronalert - Test results in app
(without total number of tests)



Coronalert - Fraction of all tests in app, fraction of tests of index cases in app, fraction of index cases who inform others by sharing keys

Glitch due to connection to EFGS

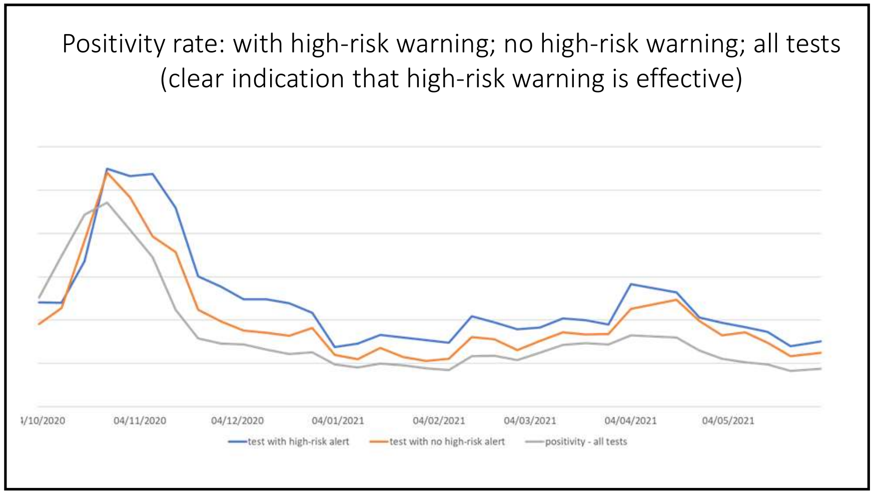
Positive impact of Covicode: more users informing others



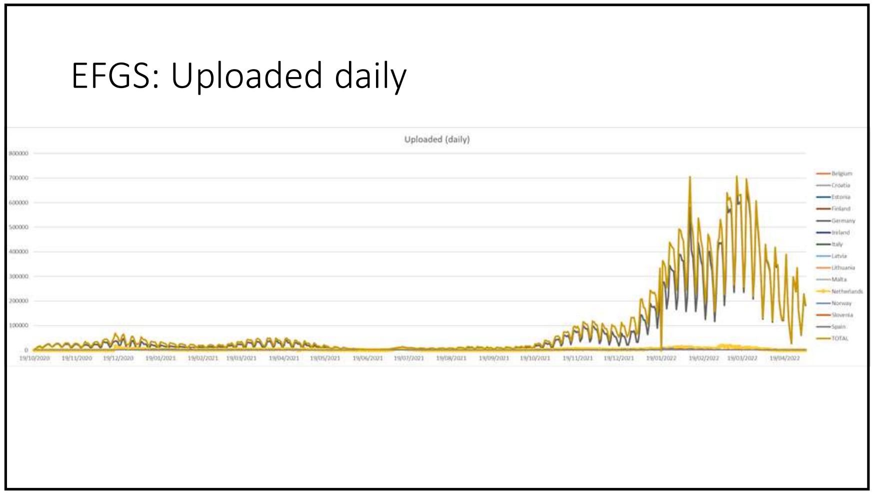
Index cases in app; index cases warning others; number of TEK keys uploaded

5 June 2022
1,754 M test results received in app
337 K positive
110 K index patients have shared 426 K keys
>250 K people have been warned (estimate)

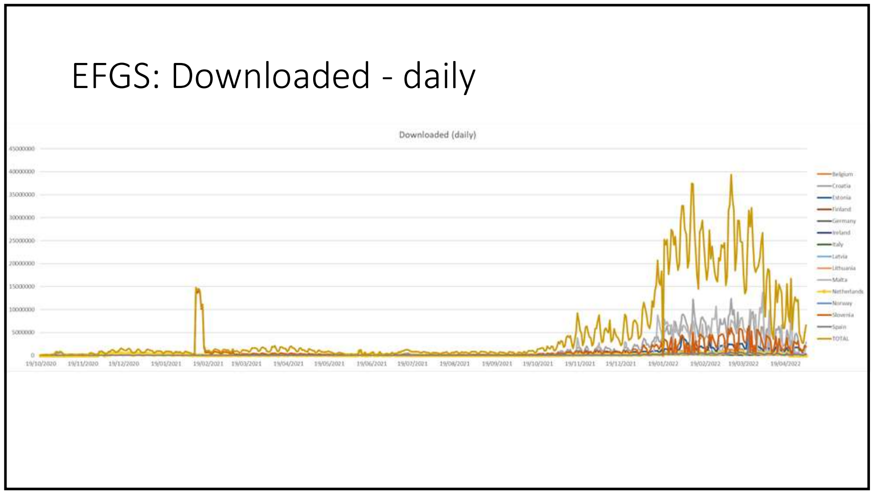
Glitch due to connection to EFGS



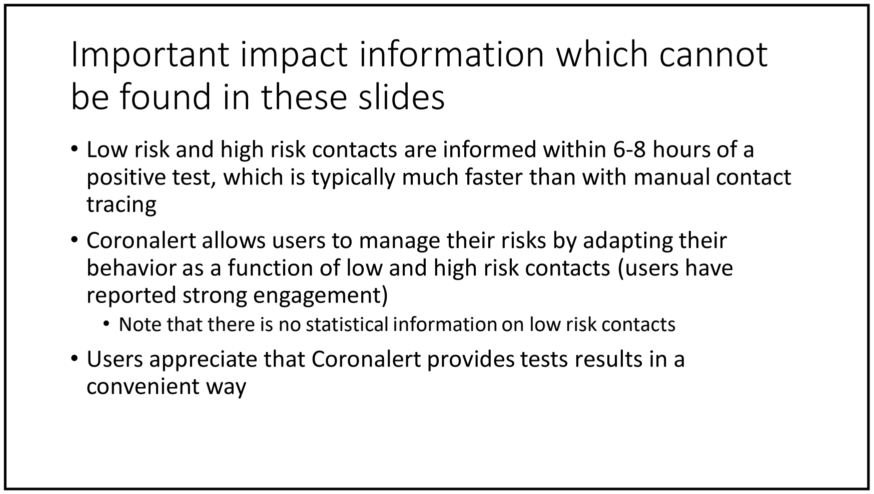
Positivity rate: with high-risk warning; no high-risk warning; all tests
(clear indication that high-risk warning is effective)



EFGS: Uploaded daily



EFGS: Downloaded - daily



Important impact information which cannot be found in these slides

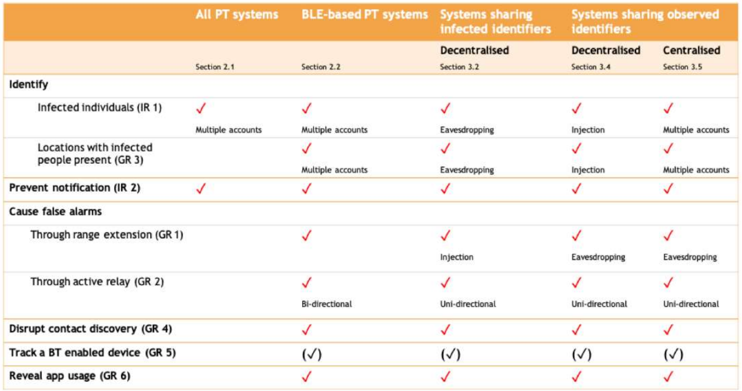
- Low risk and high risk contacts are informed within 6-8 hours of a positive test, which is typically much faster than with manual contact tracing
- Coronalert allows users to manage their risks by adapting their behavior as a function of low and high risk contacts (users have reported strong engagement)
  - Note that there is no statistical information on low risk contacts
- Users appreciate that Coronalert provides tests results in a convenient way

Is the decentralized approach a success?

- Design offers strong privacy guarantees with maximum protection against misuse of central database (at the cost of increased risk of local attacks)
- But every system (manual or digital) for contact or proximity tracing leaks information
- Effectiveness: speed, reaches new people, cannot be overwhelmed
- Can do much better but practical constraints
  - Cuckoo filters
  - BLE → UWB
  - Replay: need interaction: challenge response or Diffie-Hellman (DESIRE)
  - Relay: need location
  - [Pietrzak'20] commitment + MAC for delayed authentication – 128 vs 256 bits?
  - Some of these options create digital evidence

Generic risks for Proximity Tracing systems

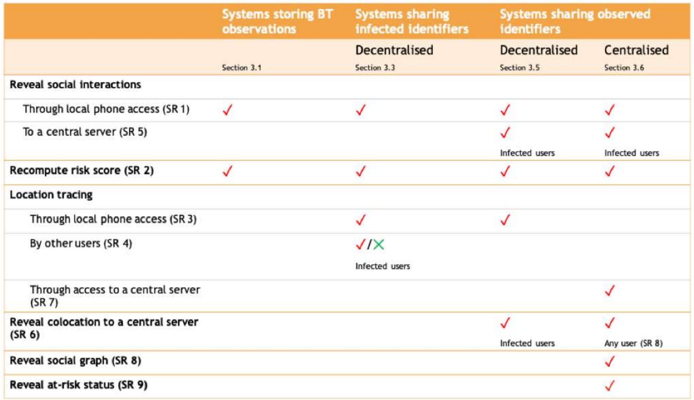
https://github.com/DP-3T/documents/



	All PT systems	BLE-based PT systems	Systems sharing infected identifiers	Systems sharing observed identifiers	
			Decentralised	Decentralised	Centralised
	Section 2.1	Section 2.2	Section 3.2	Section 3.4	Section 3.5
Identify					
Infected individuals (IR 1)	✓ Multiple accounts	✓ Multiple accounts	✓ Eavesdropping	✓ Injection	✓ Multiple accounts
Locations with infected people present (GR 3)		✓ Multiple accounts	✓ Eavesdropping	✓ Injection	✓ Multiple accounts
Prevent notification (IR 2)	✓	✓	✓	✓	✓
Cause false alarms					
Through range extension (GR 1)		✓	✓ Injection	✓ Eavesdropping	✓ Eavesdropping
Through active relay (GR 2)		✓ Bi-directional	✓ Uni-directional	✓ Uni-directional	✓ Uni-directional
Disrupt contact discovery (GR 4)		✓	✓	✓	✓
Track a BT enabled device (GR 5)		(✓)	(✓)	(✓)	(✓)
Reveal app usage (GR 6)		✓	✓	✓	✓

System-specific risks for Proximity Tracing systems

https://github.com/DP-3T/documents/



	Systems storing BT observations	Systems sharing infected identifiers	Systems sharing observed identifiers	
		Decentralised	Decentralised	Centralised
	Section 3.1	Section 3.3	Section 3.5	Section 3.6
Reveal social interactions				
Through local phone access (SR 1)	✓	✓	✓	✓
To a central server (SR 5)			✓ Infected users	✓ Infected users
Recompute risk score (SR 2)	✓	✓	✓	✓
Location tracing				
Through local phone access (SR 3)		✓	✓	
By other users (SR 4)		✓/✗ Infected users		
Through access to a central server (SR 7)				✓
Reveal colocation to a central server (SR 6)			✓ Infected users	✓ Any user (SR 8)
Reveal social graph (SR 8)				✓
Reveal at-risk status (SR 9)				✓

What were the options anyway?

- No contact tracing
- Manual contact tracing only
- Centralized proximity detection
- Decentralized proximity detection
- A beautiful high tech scheme that is more privacy-friendly and secure but that does not work on current smart phones

Each option has its own risks

Outline

- Big data and corona
- Digital proximity tracing
- Evaluation
- Presence detection

Forward tracing/presence detection: notify people who shared same indoor space

QR code?

Identify hotspots?

Current registration systems

- Privacy unfriendly:
  - data at venue, in centralized server or on smart phone in clear
- Hard to enforce
- Not easily accessible to health care workers

Privacy-friendly solutions: decentralized system and Crowd-Notifier

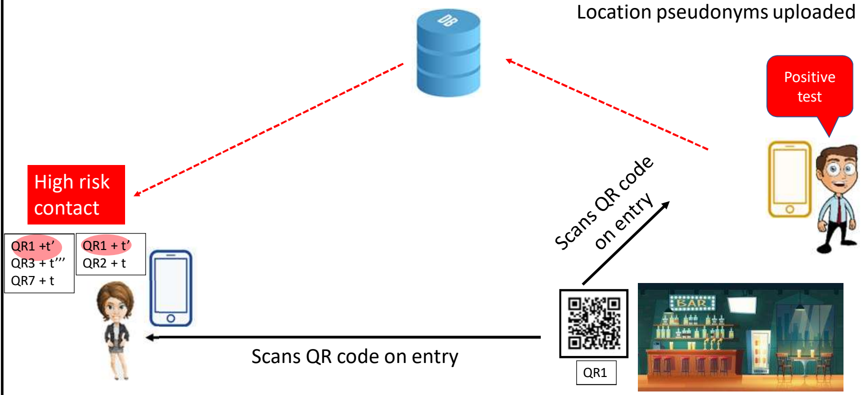
Requirements for presence tracing

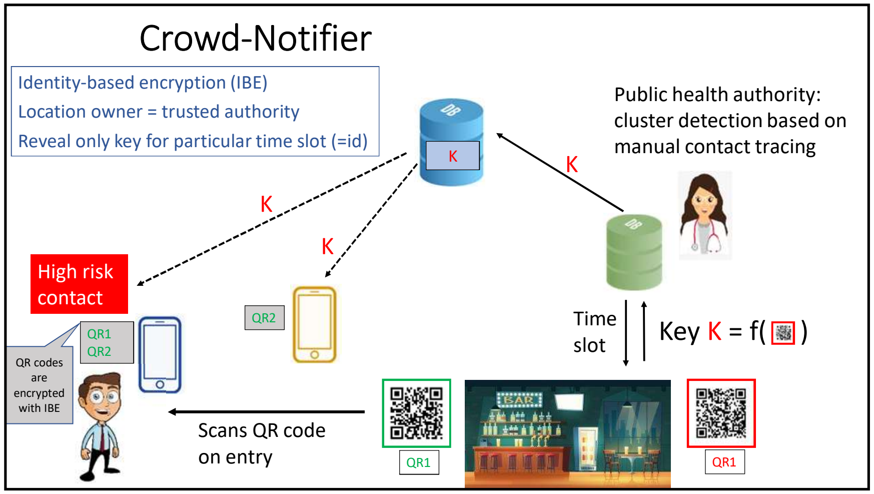
	Users	Venues	Public health authorities
privacy	No visits of venues on phone, central server or venue server	No database of venues No list of “hot” venues No profiling	
usability	Minimal effort Low battery/bandwidth All smartphones	No hardware Multiple rooms	In the loop Scalable and easy to deploy Interoperability
security	No false notifications		

Decentralized Presence Tracing

(France, Germany, UK)

Profiling of “hot” venues
Timing leaks
Sensitive info on phones
Location pseudonyms uploaded

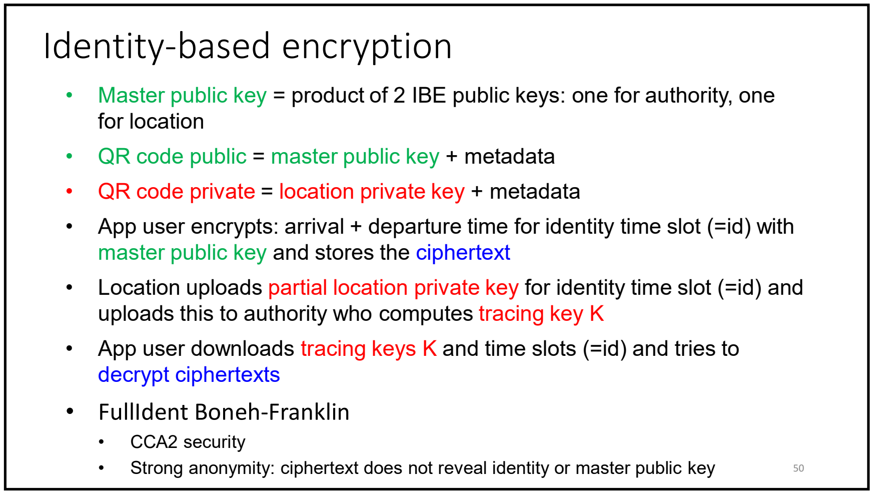




Crowd-Notifier

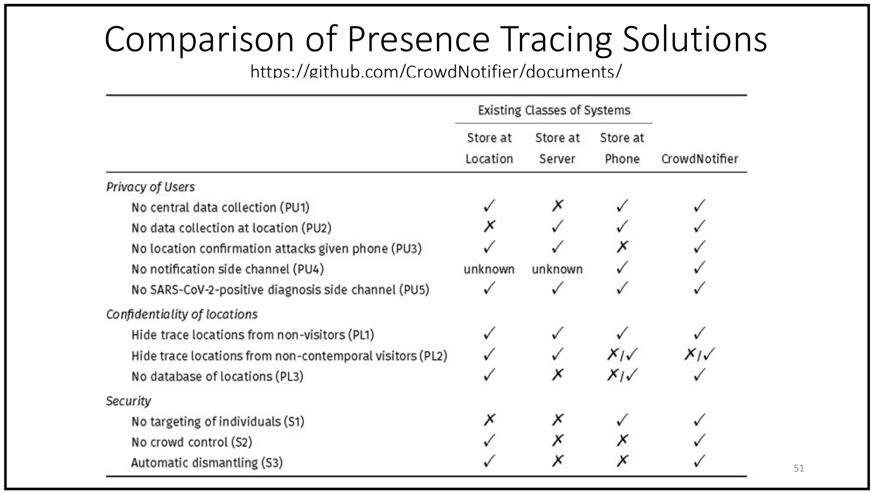
Identity-based encryption (IBE)
Location owner = trusted authority
Reveal only key for particular time slot (=id)

Public health authority: cluster detection based on manual contact tracing



Identity-based encryption

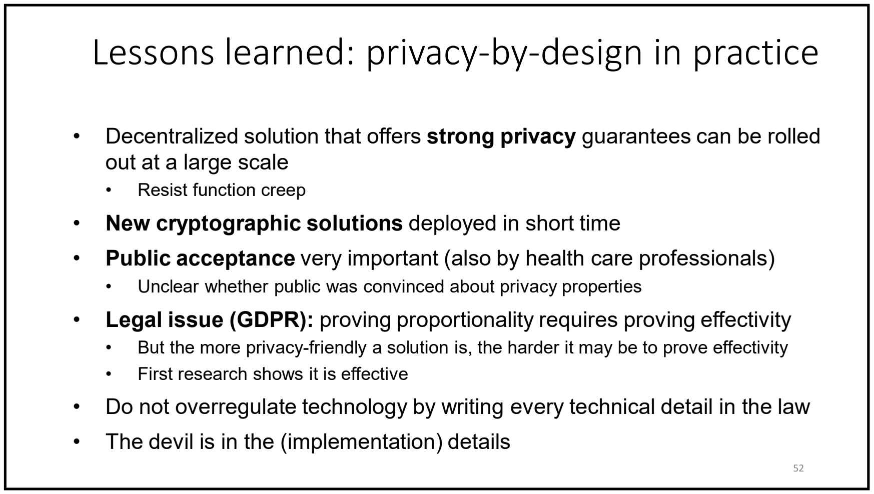
- Master public key = product of 2 IBE public keys: one for authority, one for location
- QR code public = master public key + metadata
- QR code private = location private key + metadata
- App user encrypts: arrival + departure time for identity time slot (=id) with master public key and stores the ciphertext
- Location uploads partial location private key for identity time slot (=id) and uploads this to authority who computes tracing key K
- App user downloads tracing keys K and time slots (=id) and tries to decrypt ciphertexts
- FullIdent Boneh-Franklin
  - CCA2 security
  - Strong anonymity: ciphertext does not reveal identity or master public key



Comparison of Presence Tracing Solutions

https://github.com/CrowdNotifier/documents/

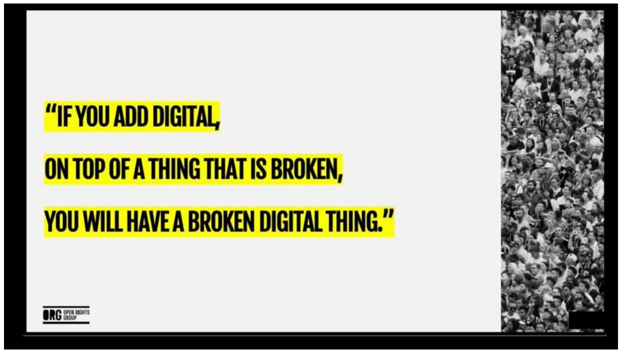
	Existing Classes of Systems			
	Store at Location	Store at Server	Store at Phone	CrowdNotifier
Privacy of Users				
No central data collection (PU1)	✓	✗	✓	✓
No data collection at location (PU2)	✗	✓	✓	✓
No location confirmation attacks given phone (PU3)	✓	✓	✗	✓
No notification side channel (PU4)	unknown	unknown	✓	✓
No SARS-CoV-2-positive diagnosis side channel (PU5)	✓	✓	✓	✓
Confidentiality of locations				
Hide trace locations from non-visitors (PL1)	✓	✓	✓	✓
Hide trace locations from non-contemporal visitors (PL2)	✓	✓	✗/✓	✗/✓
No database of locations (PL3)	✓	✗	✗/✓	✓
Security				
No targeting of individuals (S1)	✗	✗	✓	✓
No crowd control (S2)	✓	✗	✗	✓
Automatic dismantling (S3)	✓	✗	✗	✓



Lessons learned: privacy-by-design in practice

- Decentralized solution that offers **strong privacy** guarantees can be rolled out at a large scale
  - Resist function creep
- **New cryptographic solutions** deployed in short time
- **Public acceptance** very important (also by health care professionals)
  - Unclear whether public was convinced about privacy properties
- **Legal issue (GDPR):** proving proportionality requires proving effectivity
  - But the more privacy-friendly a solution is, the harder it may be to prove effectivity
  - First research shows it is effective
- Do not overregulate technology by writing every technical detail in the law
- The devil is in the (implementation) details

Lessons learned



"IF YOU ADD DIGITAL,
ON TOP OF A THING THAT IS BROKEN,
YOU WILL HAVE A BROKEN DIGITAL THING."

53

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
TELEPHONE:	+32 16 321148

54