

Digital Contact Tracing: Overview of technological solutions for the fight against pandemics

Christos Laoudias

Research Lecturer

KIOS Center of Excellence, University of Cyprus



funded by:



The COVID-19 pandemic

- The COVID-19 pandemic emerged in the late 2019 causing an unprecedented global health disruption and economic impact
- Huge pressure on Public Health Authorities
 - Hospitalization: medical personnel, ICUs, equipment, consumables
 - Monitoring: epidemiologists, tracers, health information systems¹

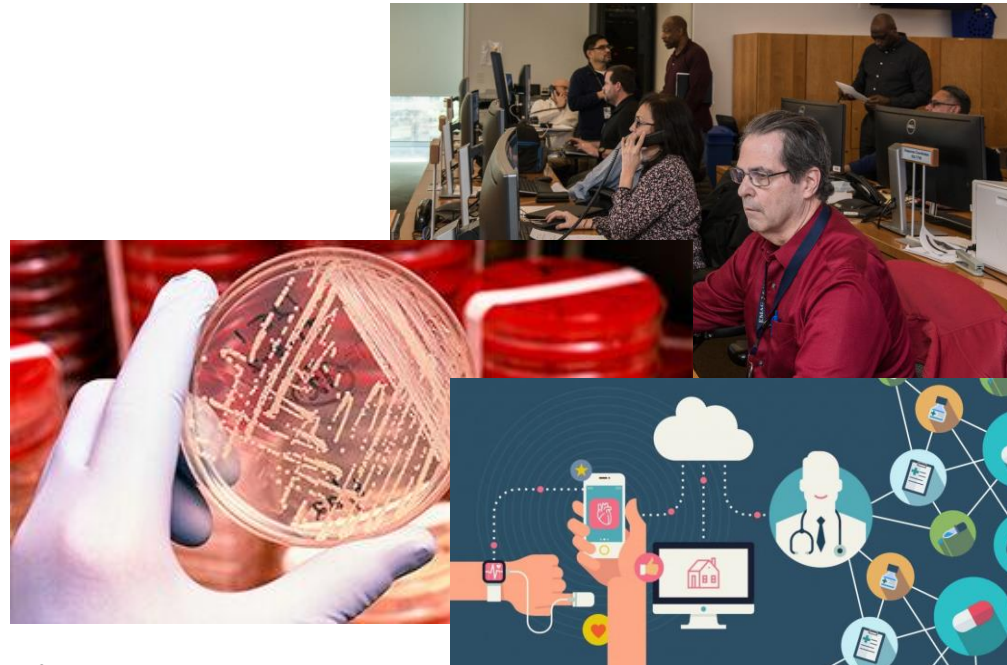


Image source: Reuters, BBC, The Guardian, CDC, ECDC, Grafimedia

¹M.N. Anastasiadou et al., A Health Information System-of-Systems for COVID-19 Pandemics Management in Cyprus, submitted to 2022 IEEE ICC E-Health Track.

Manual contact tracing



- A proven tool for managing and controlling pandemics
- If exercised by hand in large-scale with an increasing number of cases it can be a resource-hungry and inefficient process

Image source: Office of Governor Cuomo, New York, USA, Apr. 2020.

Army of contact tracers



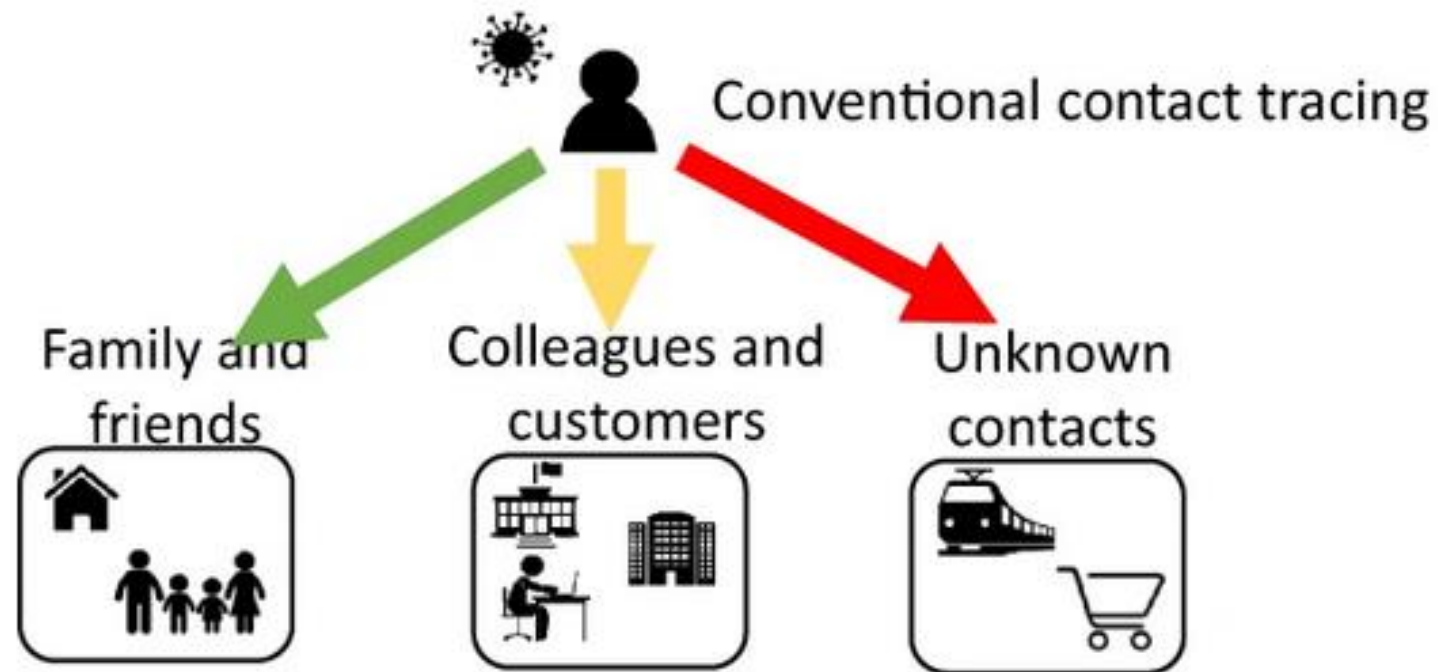
- 13K – 265K tracers estimated for USA¹
 - 100K full-time tracers for 1 year cost approx. \$3.6B
- NHS Test and Trace service (late May 2020)
 - 25K contact tracing staff
 - Capacity to trace 10K contacts per day
- Germany planned for ~21K tracers before the 2nd lockdown²

¹C. Watson, A national plan to enable comprehensive COVID-19 case finding and contact tracing in the US, Johns Hopkins Center for Health Security, 2020.

²D. Lewis, Why many countries failed at COVID contact-tracing — but some got it right, Nature News Feature, Dec. 2020.

Image source: Bryan Anselm/NYT/Redux/eyevine

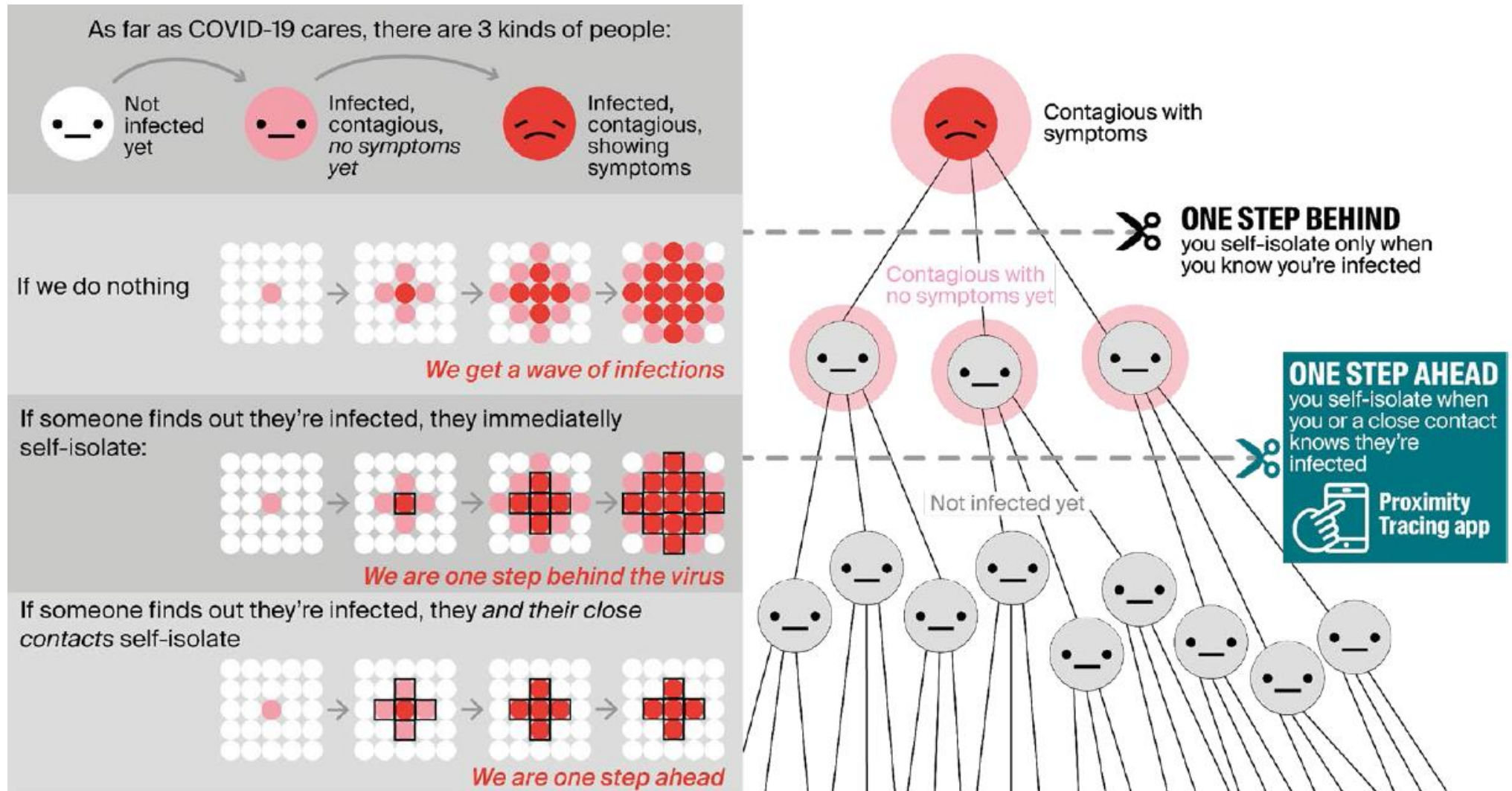
Who can be traced manually?



- Some contacts can be partly or completely missed
 - Patients' weak memory
 - Unknown contact (e.g., random encounters, nearby passengers in public transportation, in-store shopping, conference, theater, cinema, bar, etc.)
- The interview process introduces delays in notifying the contacts

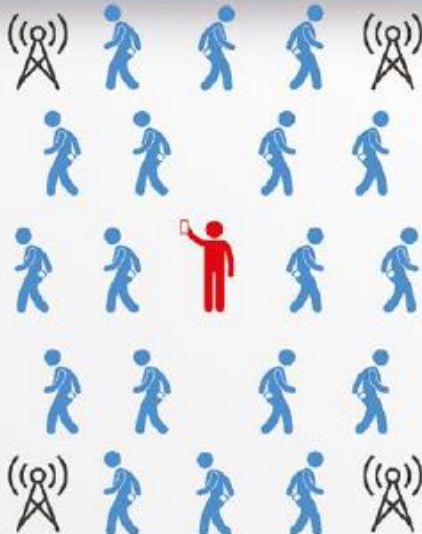

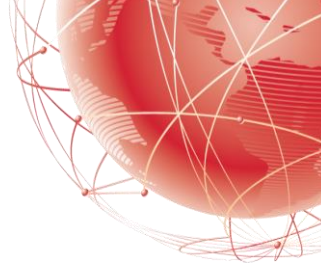
Image source: A. Elmokashfi et al., Nationwide rollout reveals efficacy of epidemic control through digital contact tracing, Nature Communications, Oct. 2021.

How can digital contact tracing help?



Source: <https://github.com/DP-3T/documents/>

Evolution of digital contact tracing





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

Use: monitoring compliance

Privacy: limited

1

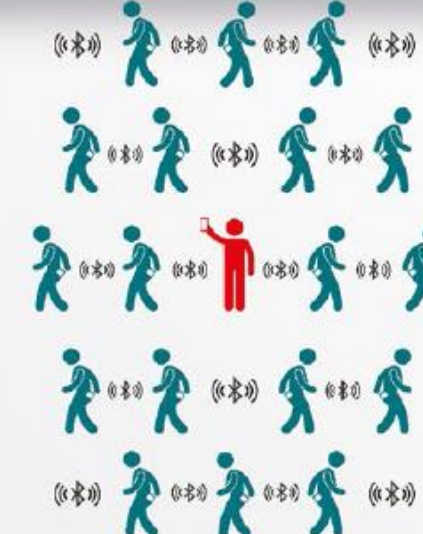



Technology: GPS location

Use: detect and avoid crowd

Privacy: citizens voluntarily give location data

2



Technology: Bluetooth anonymous exchanges

Use: one step ahead

Privacy: anonymous & privacy-preserving

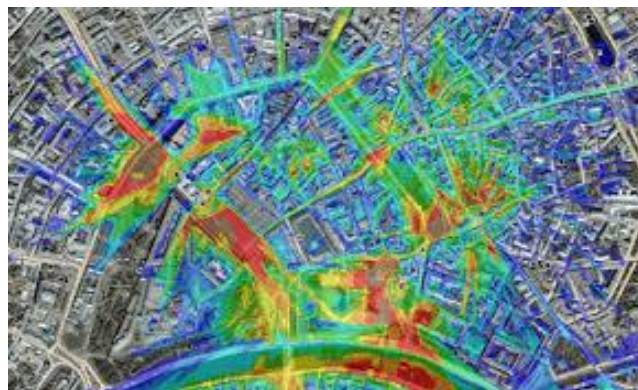
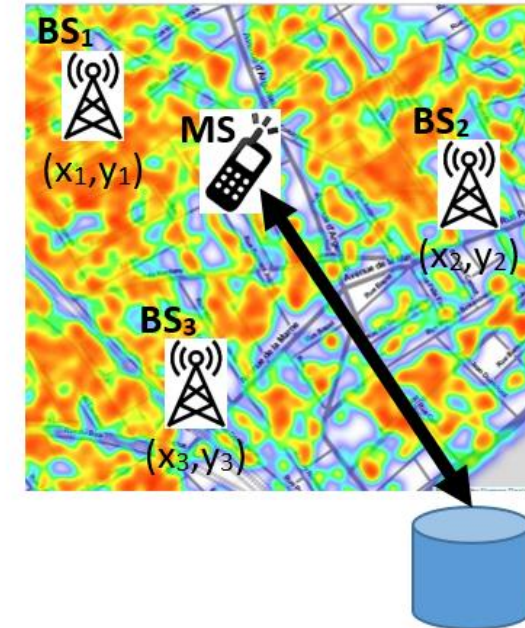
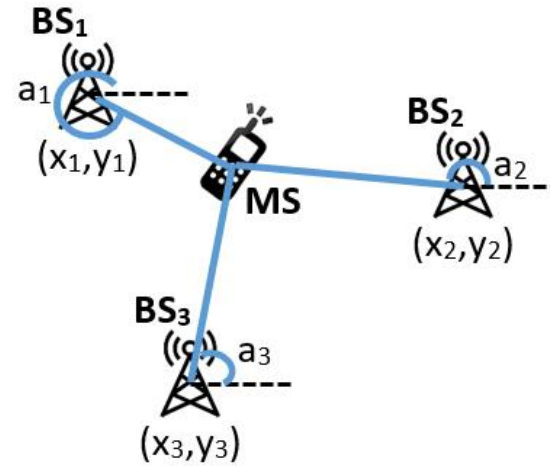
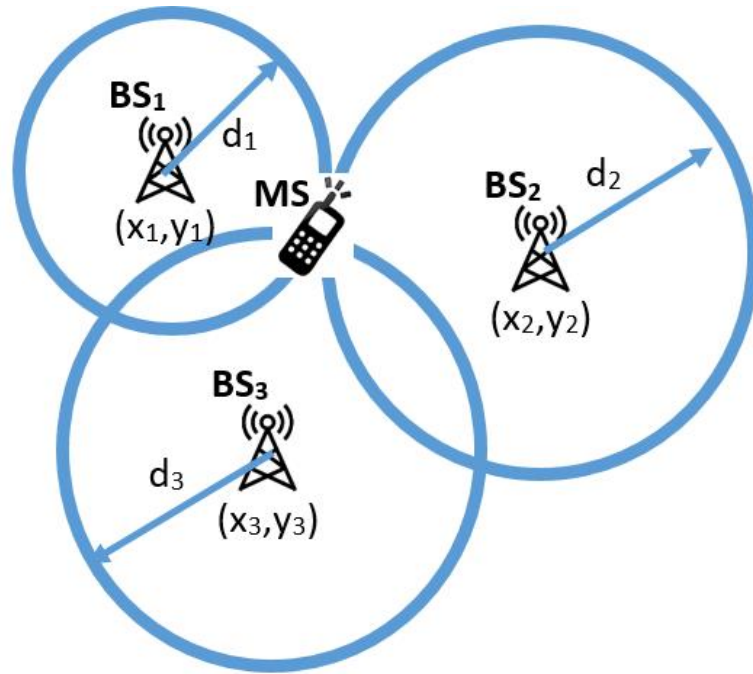
3

Centralized approach

Decentralized approach

Source: <https://github.com/DP-3T/documents/>

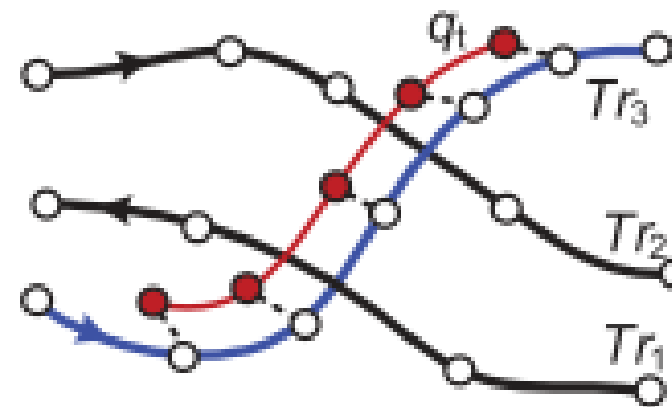
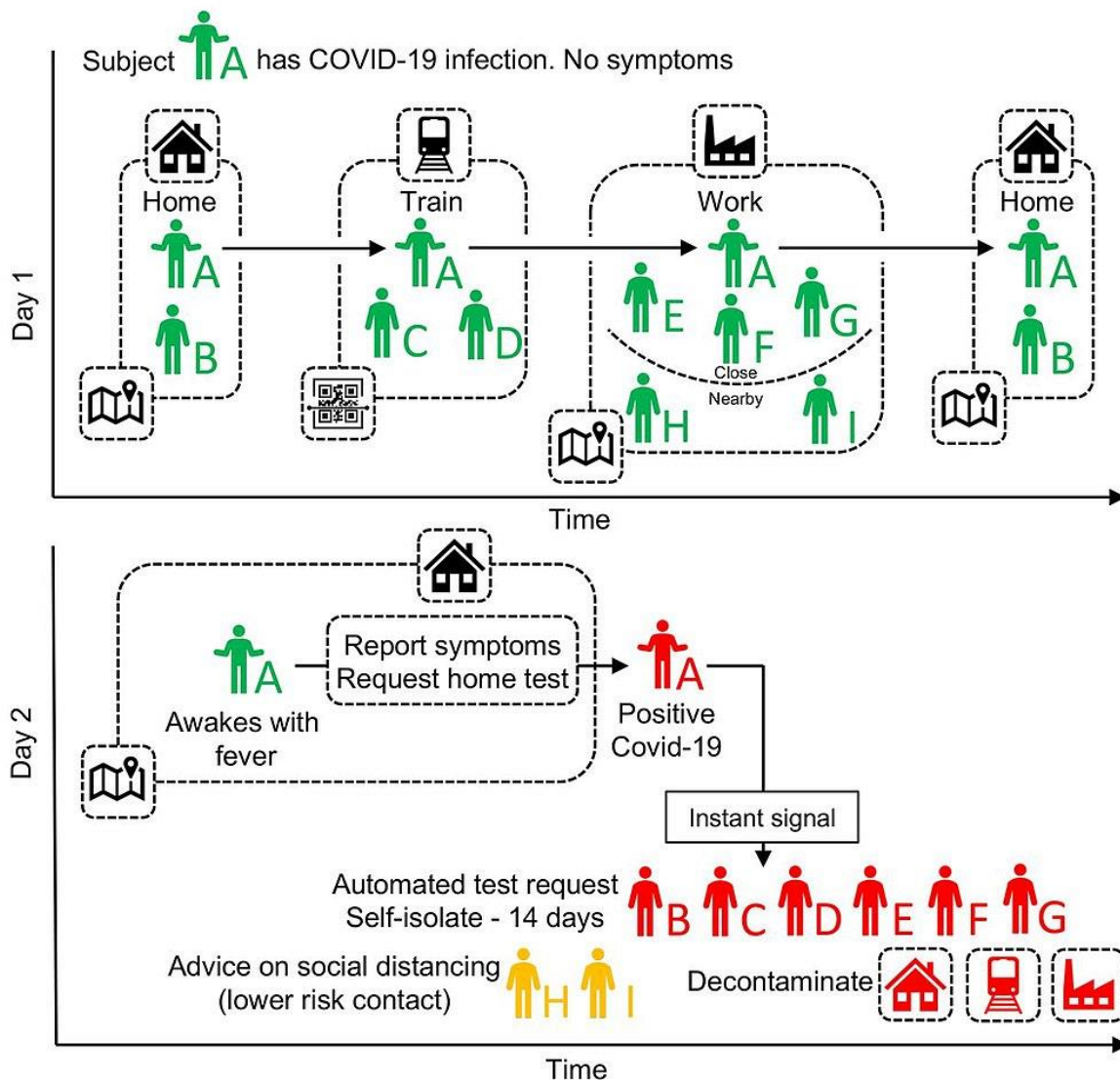
1G: Network mobile operator data



- Different ways to determine an infected user's location
 - Multilateration, triangulation, fingerprinting¹
- Health authorities can identify infection hotspots
- Limited privacy

¹C. Laoudias et al., A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation, IEEE Communications Surveys & Tutorials, 2018.

2G: GNSS location information



- 😊 Location data stored locally on the user's device unless released for tracing purposes in the case of an infection
- 😞 Still reveal to the health authorities more information (e.g., visited locations) that is necessary for contact tracing
- 😞 Limited availability indoors

Image source: L. Ferretti et al., Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science, 2020.

3G: Proximity tracing



HOW PRIVACY-FIRST CONTACT TRACING WORKS



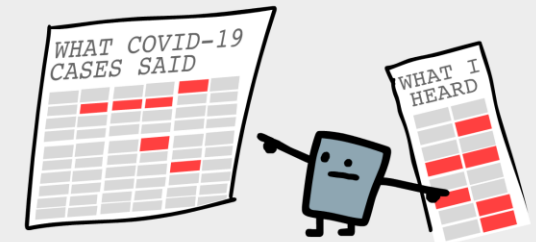
Alice's phone broadcasts a random message every few minutes.



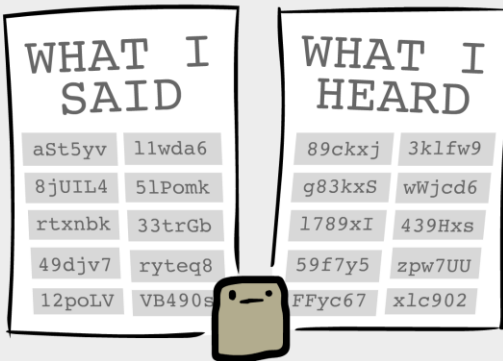
Alice sits next to Bob. Their phones exchange messages.



Because the messages are random, no info's revealed to the hospital...



...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!



Both phones remember what they said & heard in the past 14 days.



If Alice gets Covid-19, she sends her messages to a hospital.



If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.

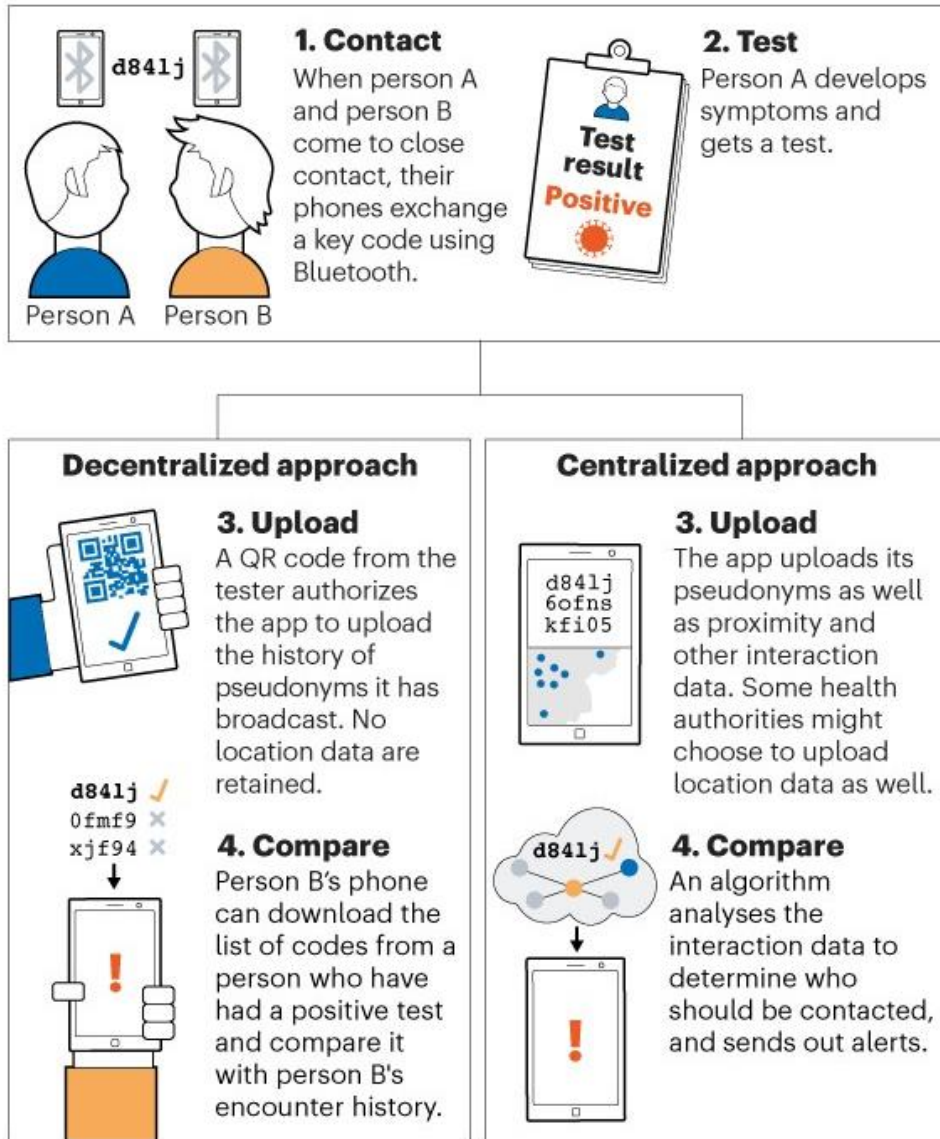


And that's how contact tracing can protect our health and privacy!

by Nicky Case (ncase.me), CC0/public domain, feel free to re-post anywhere!

Source: https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon

Centralized vs Decentralized proximity tracing



©nature

- The centralized approach can offer epidemiological insights at the expense of higher privacy risks
- Centralized approach
 - France, Hungary, Singapore, India, Australia, ...
- Decentralized approach
 - Austria, Switzerland, Estonia, Latvia, Canada, Italy, Germany, Finland, Netherlands, Ireland, Poland, Denmark, ...

Centralized vs Decentralized proximity tracing



	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

- The decentralized architecture is preferable mainly due to privacy concerns

Source: DP3T Distributed privacy-preserving contact tracing

Proximity-based protocols

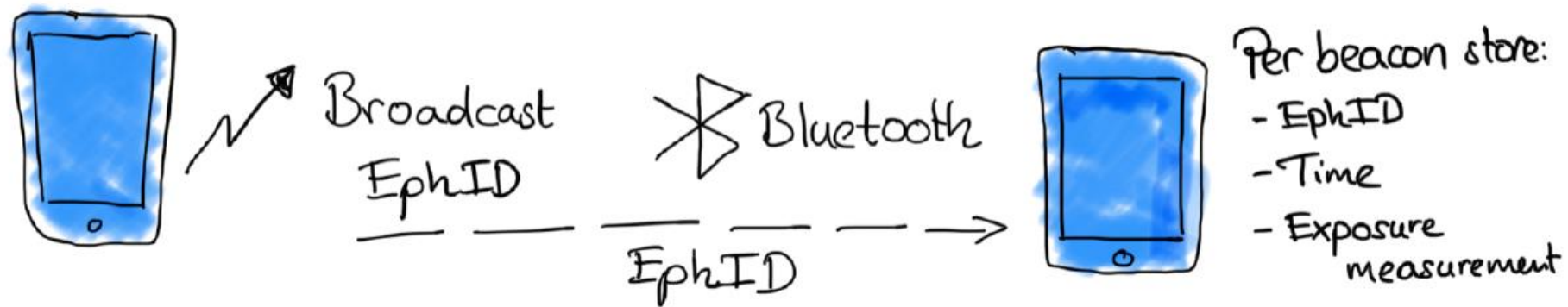


Name	Architecture	Author/promoter	Licence
Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project	Central log processing, Ephemeral IDs	Fraunhofer Institute for Telecommunications, Robert Koch Institute, Technical University of Berlin, TU Dresden, University of Erfurt, Vodafone Germany, French Institute for Research in Computer Science and Automation (Inria)	multiple protocols, closed source, private specifications
Exposure Notification	Client log processing, Ephemeral IDs	Google, Apple Inc.	public specification
Decentralized Privacy-Preserving Proximity Tracing (DP-3T)	Client log processing, Ephemeral IDs	EPFL, ETHZ, KU Leuven, TU Delft, University College London, CISPA, University of Oxford, University of Torino / ISI Foundation	publicly-developed Apache 2.0 reference implementation, MPL 2.0 iOS/Android code.
BlueTrace / OpenTrace	Central log processing, Ephemeral IDs	Singapore Government Digital Services	public specification, GPL 3 code
TCN Protocol	Client log processing, Ephemeral IDs	Covid Watch, CoEpi, ITO, Commons Project, Zcash Foundation, Openmined	publicly developed, Apache License code
Whisper Tracing Protocol (Coalition App)	Client log processing, Ephemeral IDs	Modle, Berkeley, California, TCN Coalition, French Institute for Research in Computer Science and Automation (Inria)	GPL 3
Privacy Automated Contact Tracing (East Coast PACT)	Client log processing, Ephemeral IDs	Massachusetts Institute of Technology, ACLU, Brown University, Weizmann Institute, Thinking Cybersecurity, Boston University	MIT License
Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing (West Coast PACT)	Client log processing, Ephemeral IDs	University of Washington, University of Pennsylvania, Microsoft	
NHS contact tracing protocol	Central log processing, Ephemeral IDs	NHS Digital	private specification

- Centralized: PEPP-PT, BlueTrace/OpenTrace, ROBERT, NHS protocol
- Decentralized: DP-3T, TCN, PACT, GAEN

Source: Wikipedia

Decentralized Privacy-Preserving Proximity Tracing (DP-3T)

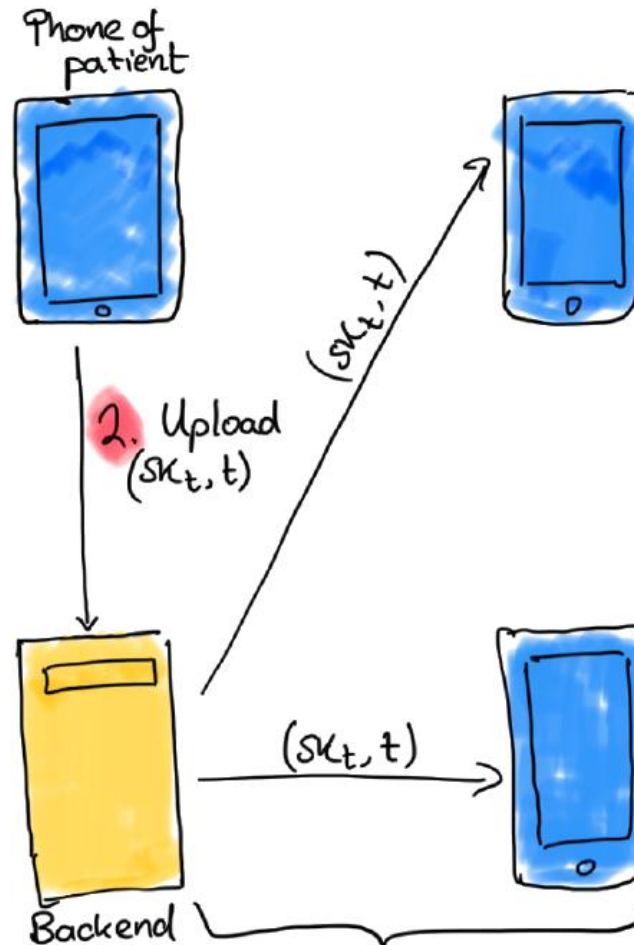
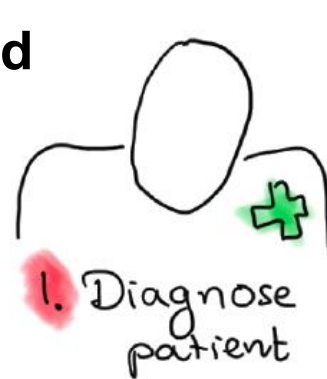


- **EphID:** Ephemeral Bluetooth identifier
 - Series of daily EphIDs created by using a secret day seed key SK_t , a pseudo-random function (e.g., HMAC-SHA256) and a pseudorandom generator (e.g. AES in counter mode)
 - Each EphID is broadcast for L minutes (i.e., epoch system parameter)
- **Time:** Day on which this beacon was received (e.g., “April 2”)
- **Exposure measurement:** e.g., signal attenuation

Source: <https://github.com/DP-3T/documents/>

Decentralized Privacy-Preserving Proximity Tracing (DP-3T)

Low-cost decentralized proximity tracing



4. Find matching beacons

- ▶ Compute $EphID_1, \dots, EphID_n$ of COVID-positive patient using SK_t
- ▶ Find all entries in local DB that match an $EphID_i$
- ▶ For each matching beacon, return
 - receive time
 - exposure measurement to the exposure estimation.



Source: <https://github.com/DP-3T/documents/>



Tech giants against COVID-19

Apple and Google partner on COVID-19 contact tracing technology

Published Apr 10, 2020

Across the world, governments and health authorities are working together to find solutions to the COVID-19 pandemic, to protect people and get society back up and running. Software developers are contributing by crafting technical tools to help combat the virus and save lives. In this spirit of collaboration, Google and Apple are announcing a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design.

Since COVID-19 can be transmitted through close proximity to affected individuals, health organizations have identified contact tracing as a valuable tool to help contain spread. A number of leading public health authorities, universities, and NGOs around the world have been doing important work to develop opt-in contact tracing technology. To further this cause, Apple and Google will be launching a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing. Given the urgent need, the plan is to implement this solution in two steps while maintaining strong protections around user privacy.

First, in May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These APIs will be available for users to download via their respective app stores.

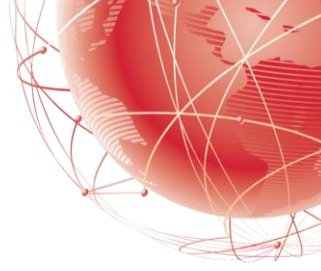


Second, in the coming months, Apple and Google will work to enable a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platforms. This is a more robust solution than an API and would allow more individuals to participate, if they choose to opt in, as well as enable interaction with a broader ecosystem of apps and government health authorities. **Privacy, transparency, and consent are of utmost importance in this effort, and we look forward to building this functionality in consultation with interested stakeholders. We will openly publish information about our work for others to analyze.**

All of us at Apple and Google believe there has never been a more important moment to work together to solve one of the world's most pressing problems. Through close cooperation and collaboration with developers, governments and public health providers, we hope to harness the power of technology to help countries around the world slow the spread of COVID-19 and accelerate the return of everyday life.

- Exposure Notifications Express
- Raised a lot of controversy

Google Apple Exposure Notification (GAEN)



What Apple and Google have proposed



When A and B meet, their phones exchange a key code



When A becomes infected, he updates his status in the app and gives his consent to share his key with the database



B's phone regularly downloads the database to check for matching codes. It alerts her that somebody she has been near has tested positive

- Cross-device interoperability: Works seamlessly between Android and iPhones
- Secure Bluetooth scanning and message exchange with nearby devices
 - AES128-based encryption
- Similar to DP-3T and TCN protocols
 - 16-byte random day Temporary Exposure Key (TEK), Rolling Proximity Identifier (RPI), ...
- Implemented at the OS level through an API
 - More efficient operation as a background process
- Decentralized exposure risk score calculation

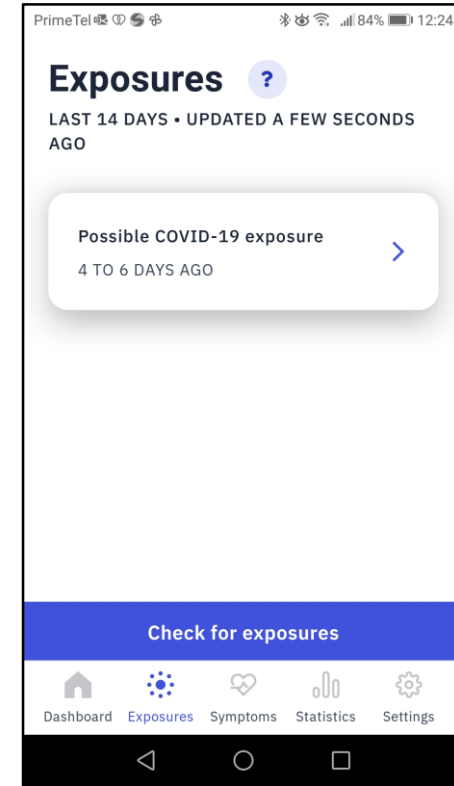
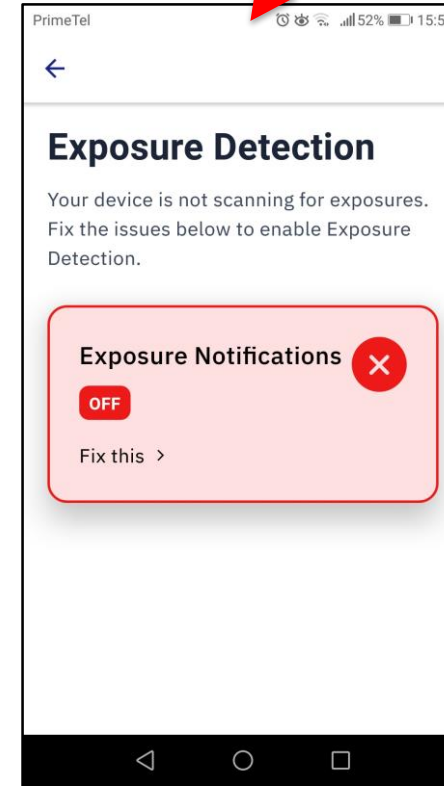
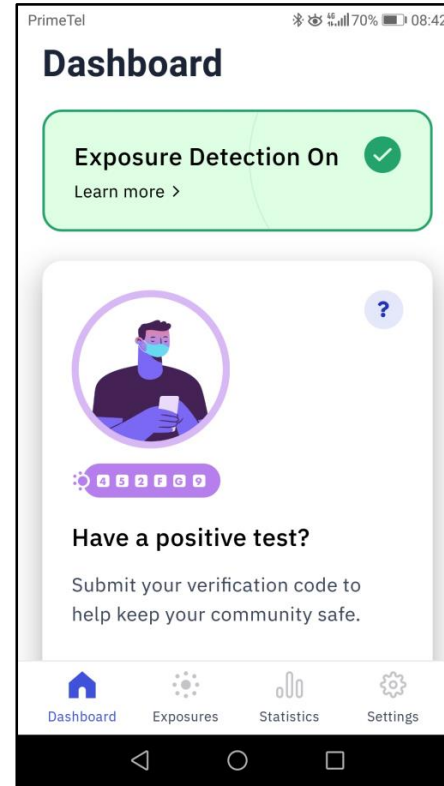
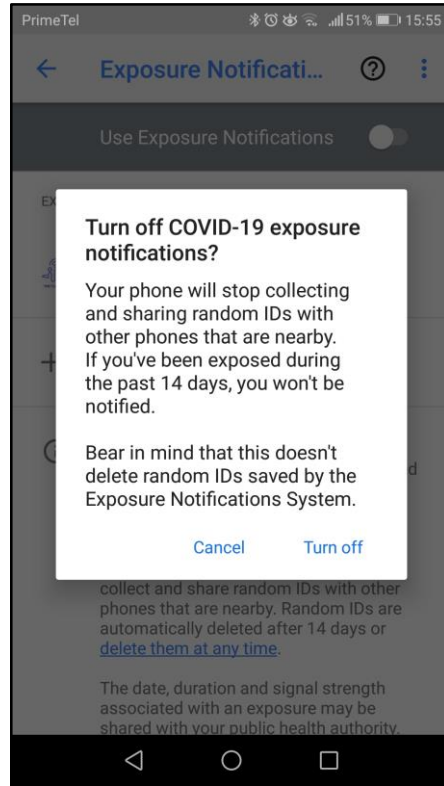
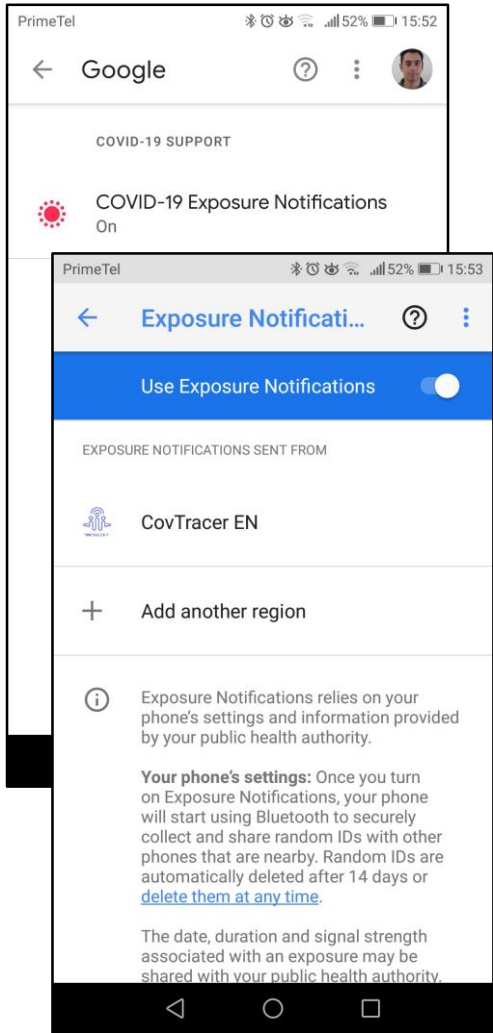
Source: Apple/Google

BBC

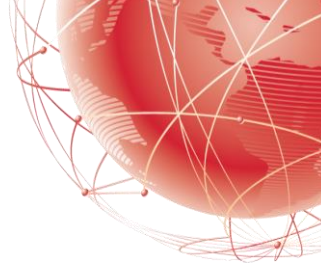
GAEN in action



No Bluetooth

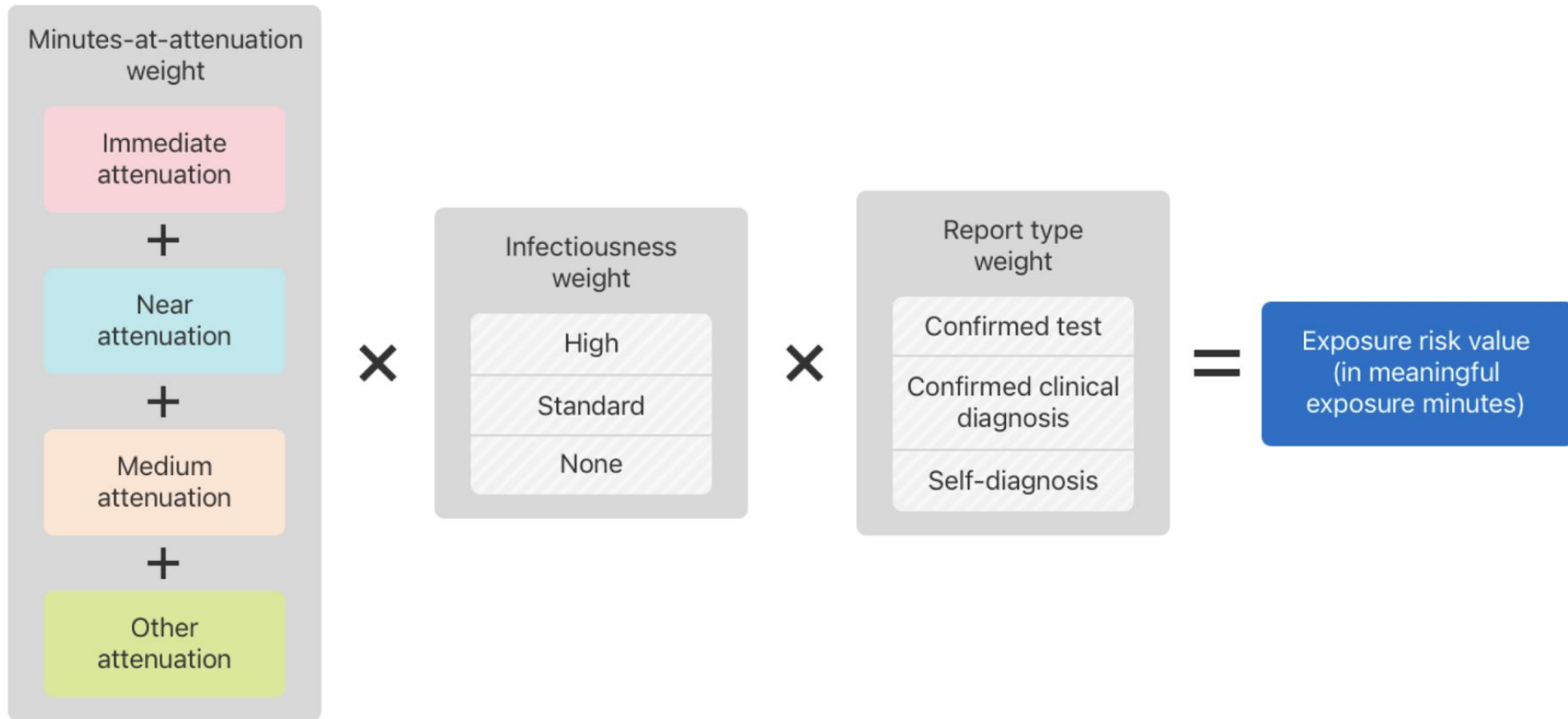


- In early versions, Bluetooth was under the Google Location services and decoupled later



How is the risk score calculated?

- Risk score function: Combination of 3 weights



Source: Linux Foundation Public Health (LFPH)

Image source: <https://developer.apple.com/documentation/exposurenotification/enexposureconfiguration>

Configuring Bluetooth attenuations



		Immediate	Near	Medium	Other	
Narrower Net	<i>Threshold</i>	<55 dB	<63 dB	<70 dB	--	<53dB; <62dB; <70dB
	<i>Weight</i>	150%	100%	40%	0%	
Wider Net	<i>Threshold</i>	<55 dB	<70 dB	<80 dB	--	
	<i>Weight</i>	200%	100%	25%	0%	

- Narrower Net prioritizes **specificity** → **Fewer notifications** are triggered
 - Captures some fraction of close contacts and limits the number of further-distance exposures captured
- Wider Net prioritizes **sensitivity** → **More notifications** are triggered
 - Captures most close-contact exposures and a non-negligible amount of further-distance exposures

Source: <https://github.com/lfph/gaen-risk-scoring/blob/main/risk-scoring.md>

Configuring infectiousness

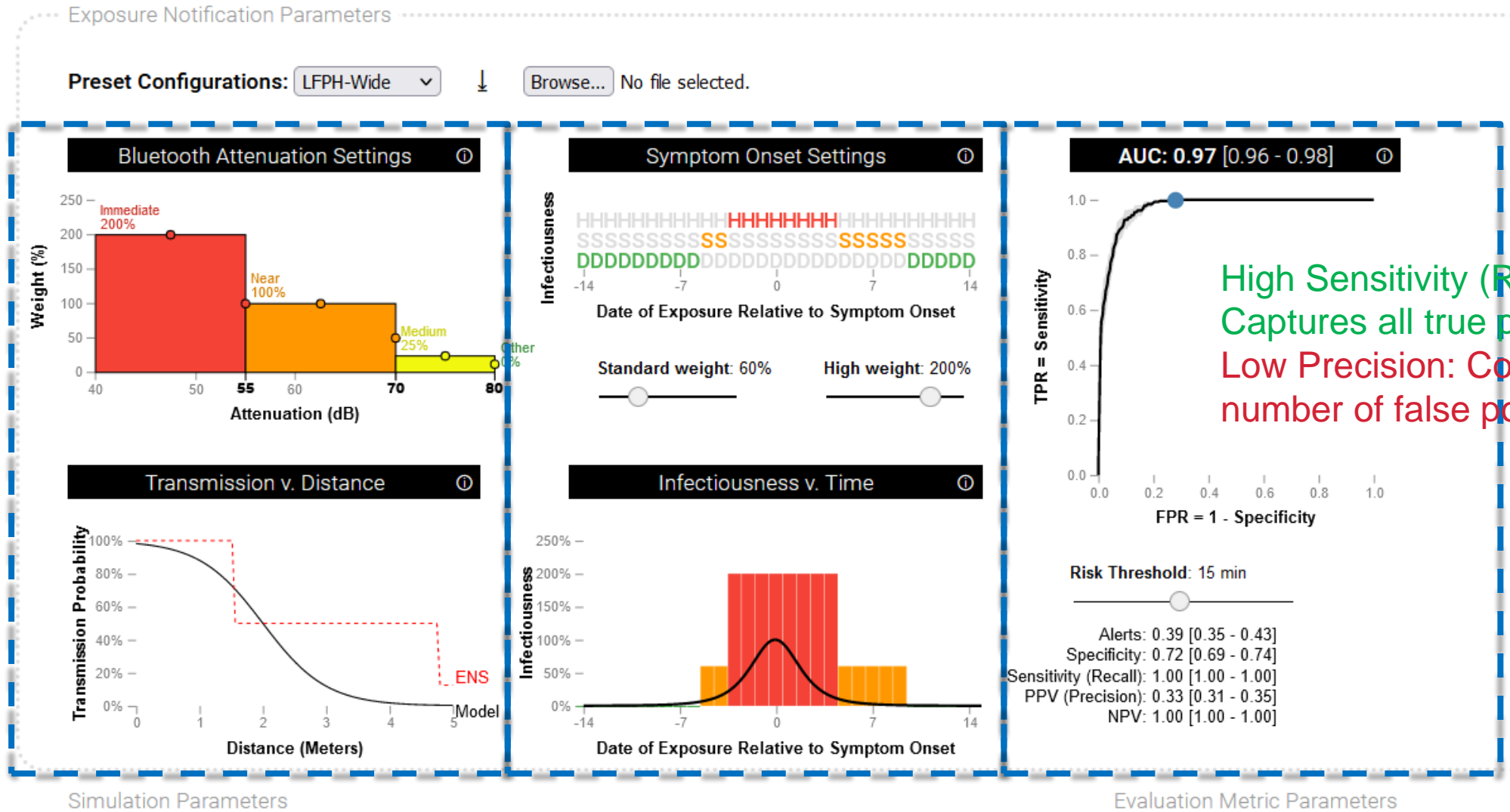


	Narrower net	Wider net
Symptom Onset Map	<i>None: days -14 to -4; days +5 to +14</i> <i>Standard: day -3; day +4</i> <i>High: days -2 to +3</i>	<i>None: days -14 to -6; days +10 to +14</i> <i>Standard: -5 to -4 days; days +5 to +9</i> <i>High: days -3 to +4</i>
Standard weight	30%	60%
High weight	100%	200%

- Narrower Net prioritizes **specificity**
 - **Fewer notifications** restricting to exposures during the period of peak infectiousness
- Wider Net prioritizes **sensitivity**
 - **More notifications** capturing exposures over a longer period of potential infectiousness

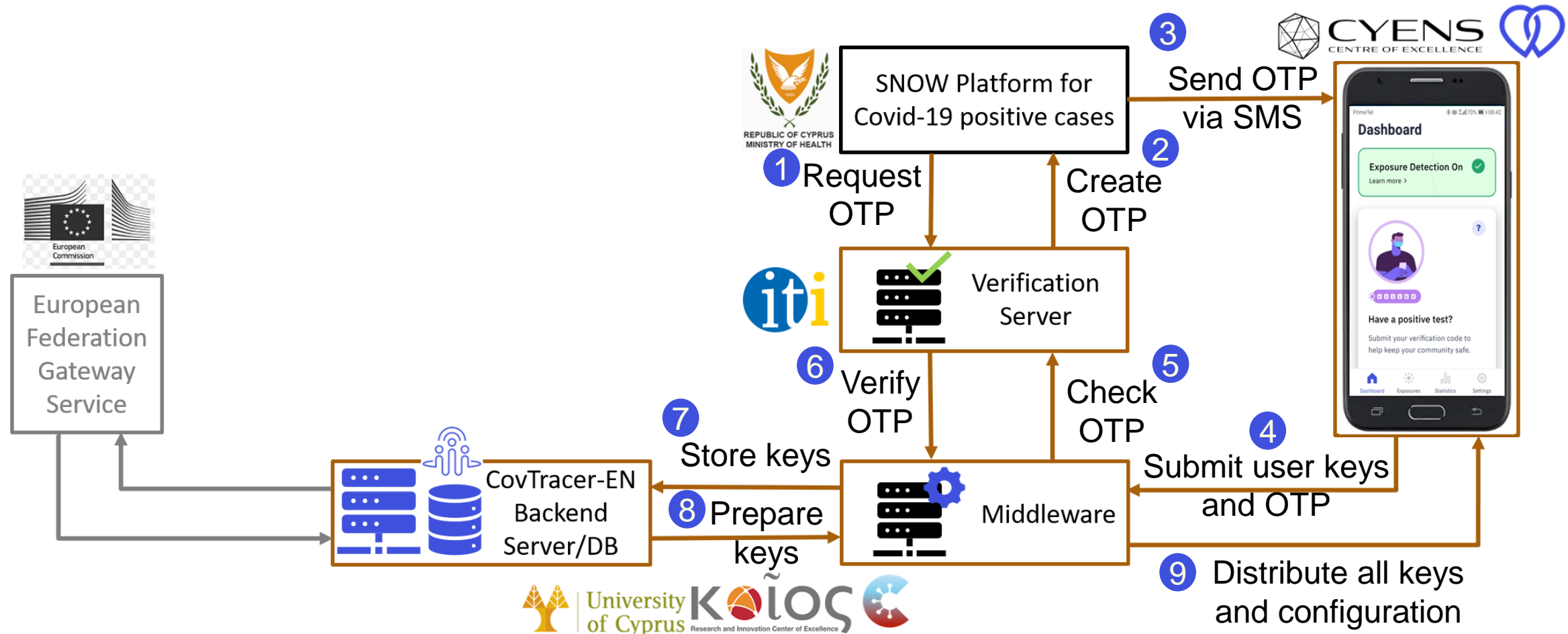
Source: <https://github.com/lfph/gaen-risk-scoring/blob/main/risk-scoring.md>

COVID-19 Risk Score Tuner – Wider net



Source: Murphy, K., Kumar, A. and Serghiou, S., 2021. Risk score learning for COVID-19 contact tracing apps. arXiv preprint arXiv:2104.08415.
<https://risk-score-tuner.appspot.com/>

Integration with the contact tracing ecosystem



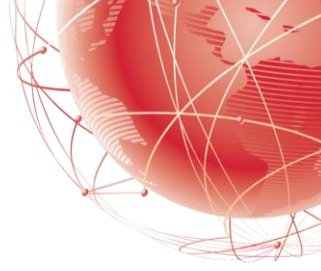


Uptake of GAEN-based apps

- UK's NHS COVID-19 app
 - By end of Oct. 2020, the NHS COVID-19 app was downloaded by more than 19M users, i.e., more than **40%** of adults with access to a compatible smartphone
 - In Autumn-Winter 2020 it was used regularly by approximately 16.5M users, i.e., **28%** of the total population
 - At the end of 2020, it was the 2nd most-downloaded free app in the UK in Apple App store (behind Zoom and above TikTok)
- By end of Nov. 2021, 69 territories have deployed GAEN-based apps¹
 - 26 states in the USA
 - 24 European countries (Scotland and Northern Ireland operate separate apps)
 - 17 other countries around the world (e.g., Canada, Brazil, Japan)
- Common EU Toolbox for Member States regarding mobile applications to support contact tracing [eHealth Network]
 - Facilitate and support the development, release, and uptake of national apps

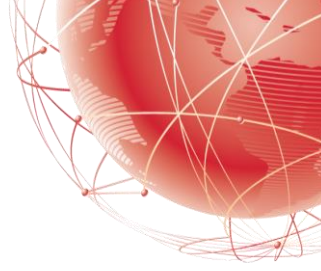
¹Source: <https://developers.google.com/android/exposure-notifications/apps>

Uptake across EU Member States



- 21 EU Member States operate a national contact tracing app
 - Decentralized GAEN-based (19), Centralized (2)
 - The Czech Republic app (eRouška) was recently paused
 - ~27% of EU citizens (~110M) have downloaded their national app (max: 56%)
- Why not a single pan-European contact tracing app?
 - Allow State-specific integration with national public health system/processes
 - What happens when EU citizens start traveling across Europe?

EU guidelines for app interoperability



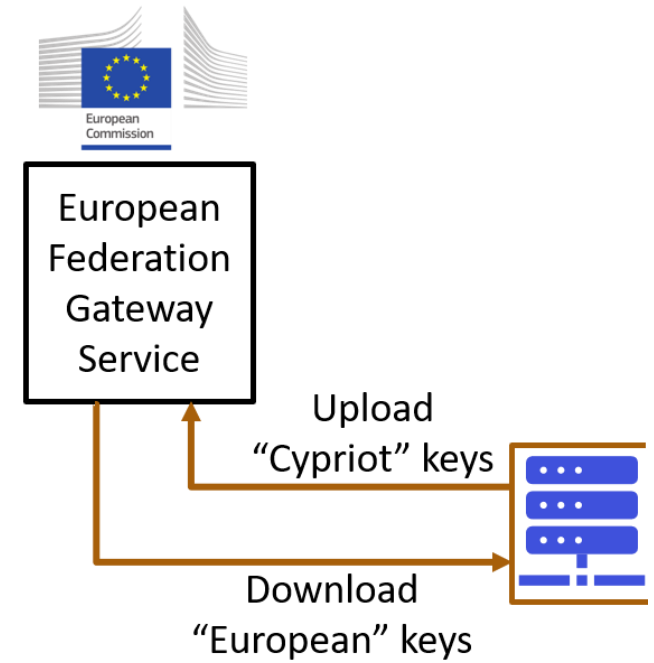
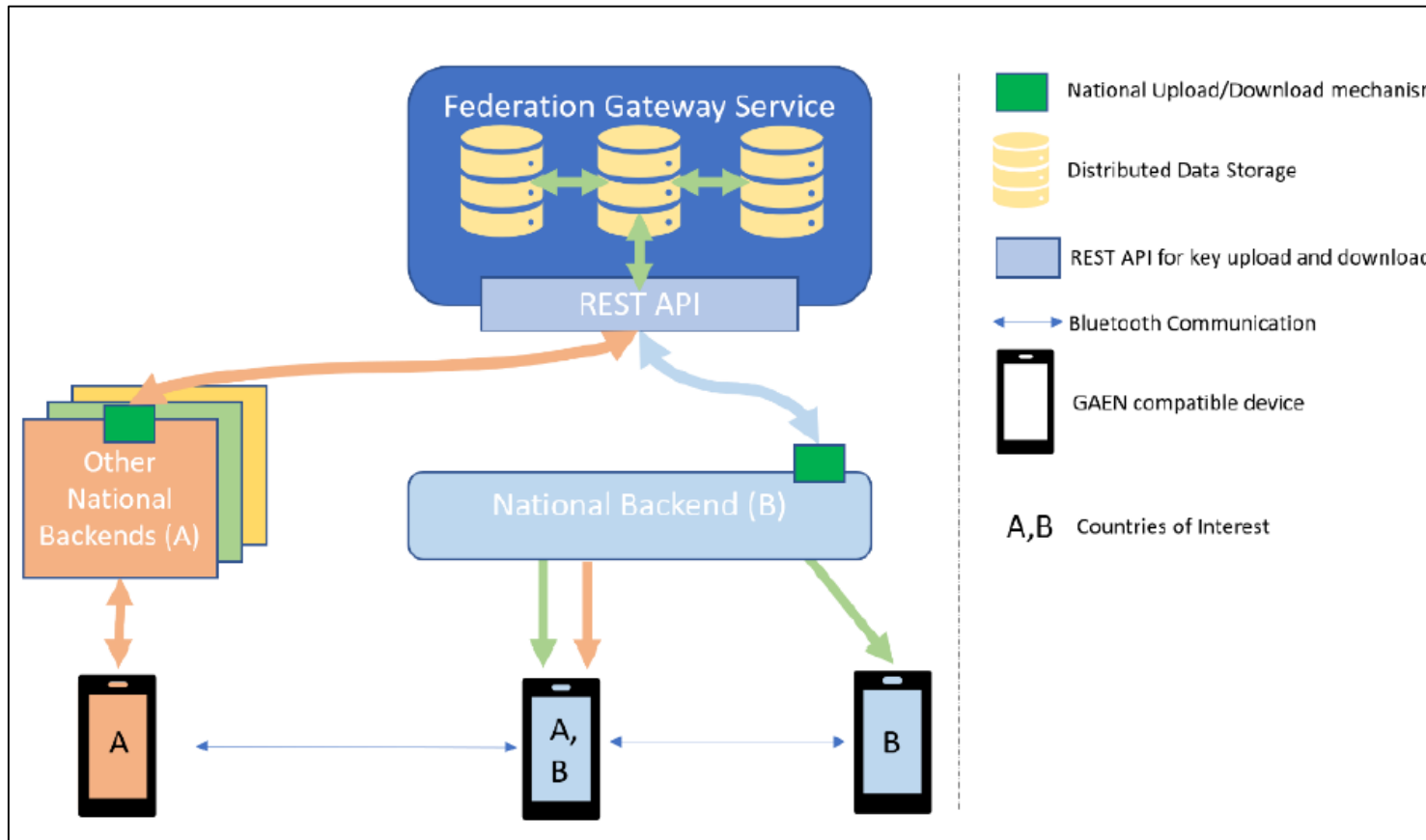
- Guidelines
 - Tracing apps must be voluntary, transparent, secure, **interoperable** and respect people's privacy
 - Apps will use arbitrary identifiers, no geolocation or movement data will be used
 - All apps have to be temporary only, so they will have to be dismantled as soon as the pandemic is over
 - Apps should function **everywhere in the EU, across borders** and across operating systems
- Why are such guidelines needed?
 - Enable wide, voluntary take-up of national tracing apps
 - Facilitate the **tracing of cross-border infection chains**, be valuable for **cross-border workers, tourism, business trips** and **neighbouring countries**
 - Support the relaxing of confinement measures, the **gradual lifting of border controls**, and the restoration of freedom of movement **throughout the EU**

Source: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_869

Cross-border interoperability scenario



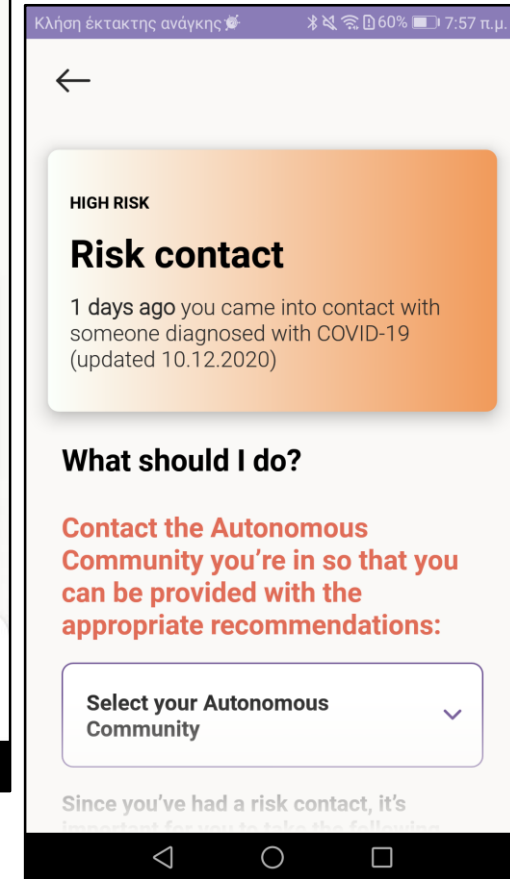
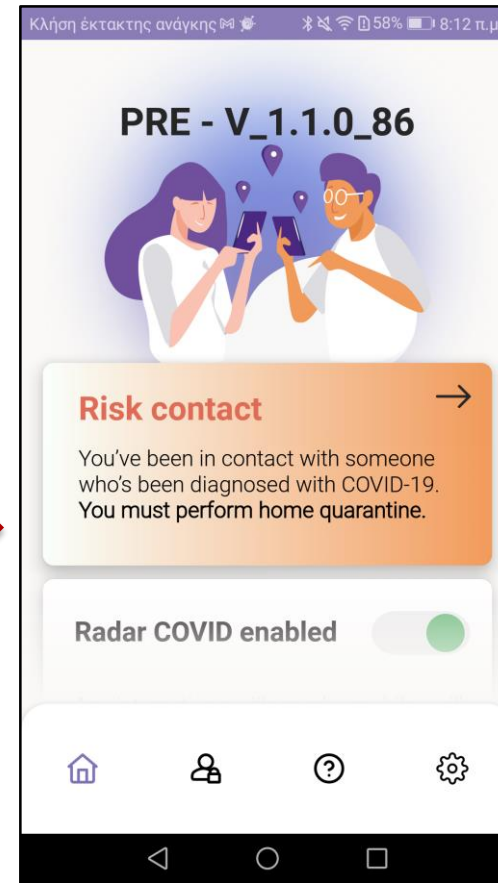
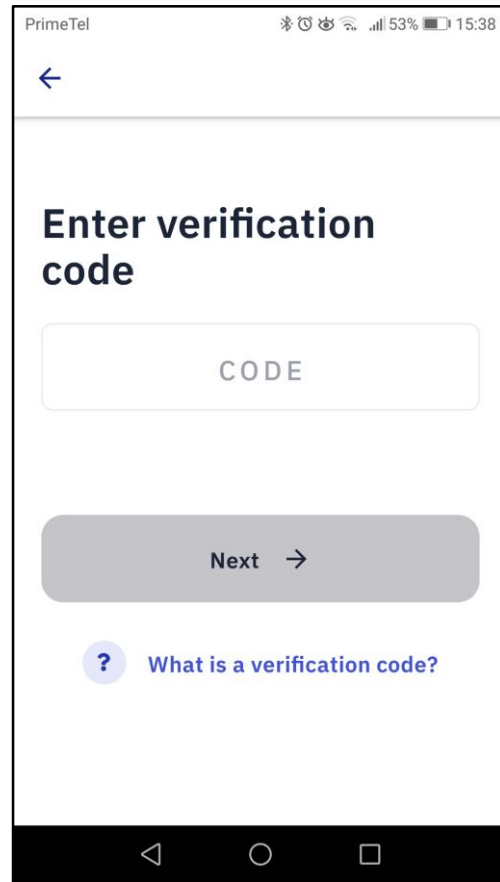
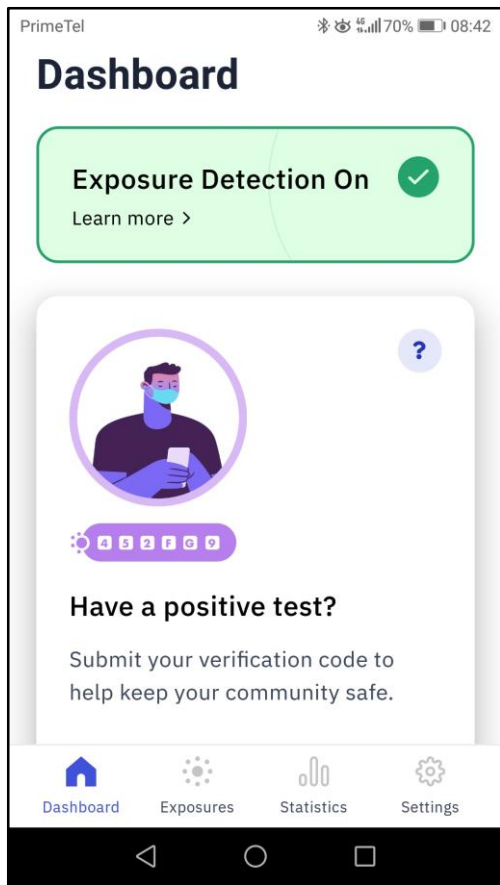
European Federation Gateway Service (EFGS)



- Facilitates backend-to-backend integration and countries can onboard incrementally
- National backends retain flexibility and control over data distribution to their users
- Enables national apps to talk to each other → contact tracing “roaming”

Source: eHealth Network, Interoperability specifications for cross-border transmission chains between approved apps v1.0, Jun. 2020

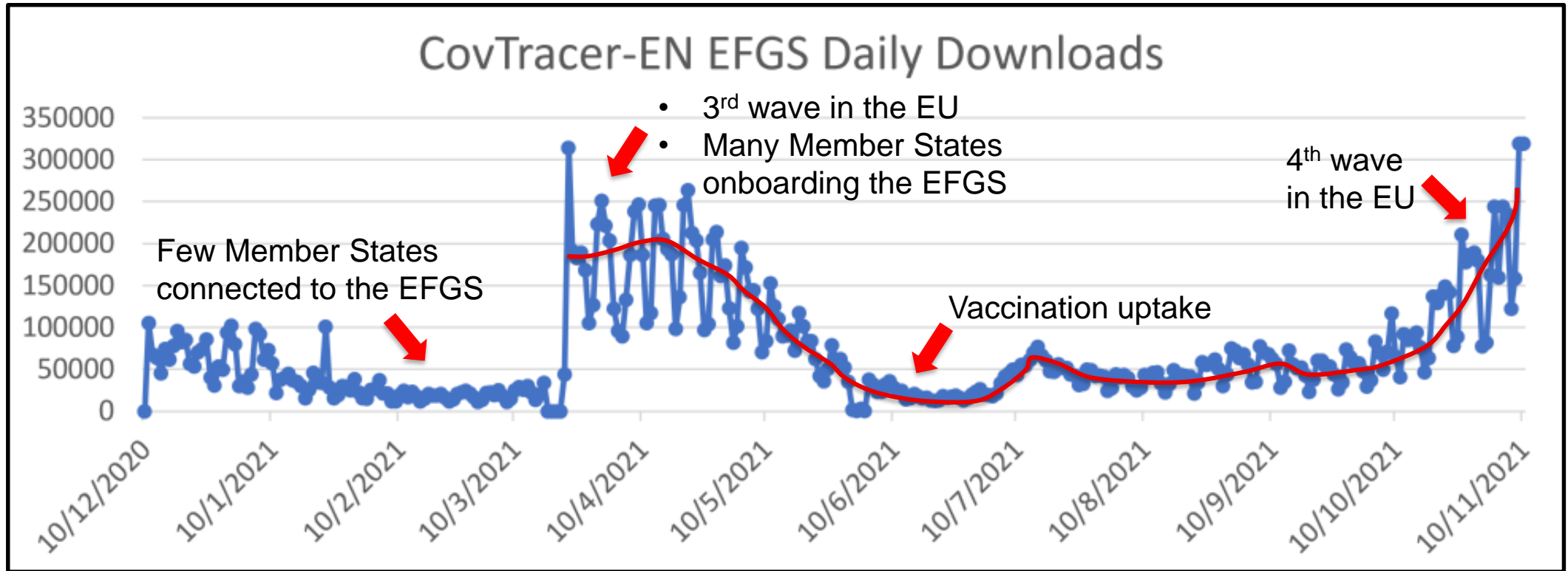
Cross-border interoperability verification





Statistics from the EFGS

- 18 EU Member States have joined the EFGS since Oct. 2020
 - The Czech Republic recently disconnected



Source: Key traffic of the European Federation Gateway Service (EFGS) retrieved from data.europa.eu



Effectiveness of contact tracing apps

- Misconception from early studies that high adoption rates are needed (e.g., **56%** of the total population) to be effective¹
- Modeling in Washington state [USA, September 2020]²
 - Modeling by Google & Oxford University
 - With 15% of the population participating, apps could reduce infections and deaths by approximately **8%** and **6%** (combined with traditional contact tracing and social distancing)
- Study in Arizona State University [USA, autumn 2020]³
 - 46% of infected persons interviewed had the app and 55% of these app users shared their positive test result
 - Apps could reduce the rate of infection R by **~12%** and would be a significant contribution to transmission control

¹R. Hinch et al., Effective configurations of a digital contact tracing app: a report to NHSX, Aug. 2020. https://github.com/BDI-pathogens/covid-19_instant_tracing

²M. Abueg et al., Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state, MedRxiv, Sep. 2020.

³J. Masel et al., Quantifying meaningful adoption of a SARS-COV-2 exposure notification app on the campus of the university of arizona, medRxiv, Oct. 2021.

Effectiveness of contact tracing apps



- Smittestopp (non-GAEN version) [Norway, spring 2020]¹
 - The tracing efficacy (i.e., the probability that a physical proximity event between two phones is detected by the app) was measured at **80%**
 - At least **11%** of the discovered close contacts could not have been identified by manual contact tracing
 - Significant impact even for moderate uptake numbers (e.g., 40% for $R=1.5$)
- Radar Covid [Spain, summer 2020]²
 - 4-week population-based controlled experiment in La Gomera (Canary Islands)
 - 7 KPIs: 5 for user behaviour (*adoption, adherence, compliance, turnaround time, follow-up*) and 2 for effectiveness (*overall detection, hidden detection*)
 - At least 33% of the population adopted the technology, 349 simulated infections
 - **6.3** close-contacts detected per primary simulated infection, a significant percentage being contacts with strangers (~3 manually traced contacts in Spain)

¹A. Elmokashfi et al., Nationwide rollout reveals efficacy of epidemic control through digital contact tracing, Nature Communications, Oct. 2021.

²P. Rodríguez et al., A population-based controlled experiment assessing the epidemiological impact of digital contact tracing, Nature Communications, Jan. 2021.



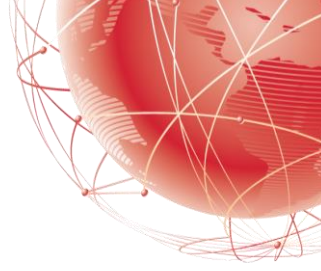
Effectiveness of contact tracing apps

- NHS COVID-19 [England and Wales, autumn-winter 2020]¹
 - 1.7M notifications sent, i.e., ~4 per positive case consenting to contact tracing
 - **6%** of individuals notified by the app subsequently showed symptoms and tested positive (i.e., secondary attack rate) that is similar to manual contact tracing
 - For every 1% increase in app users, the number of infections can be reduced by **0.8%** (modelling) or **2.3%** (statistical analysis)
 - Public Health message is clear: ‘Use the app, it works’.
- Corona-Warn-App [Germany, spring 2021]²
 - Event-Driven User Survey (EDUS) and Privacy-Preserving Analytics (PPA)
 - 73% were surprised to have received a ‘red’ warning (increased risk) [EDUS]
 - **~6%** of the tests carried out as a result of a (red) warning were positive [EDUS]
 - Users who share positive test results warn around six other users [PPA]

¹C. Wymant et al., The epidemiological impact of the NHS COVID-19 App, Nature, May 2021.

²About the Effectiveness and Benefits of the Corona-Warn-App, Jun. 2021 <https://www.coronawarn.app/en/science/2021-06-15-science-blog-1/>

Effectiveness of contact tracing apps



- SwissCovid [Switzerland, June 2021]¹
 - Contributed to preventive actions in **76%** of exposure notification recipients and were associated with a faster quarantine time in some user groups
 - Estimated to have contributed to the notification and identification of 500 to 1000 positive app users per month (lower than UK and Germany)
- Study by the Civil Liberties Union for Europe [October 2021]²
 - Examined 10 EU Member States on the impact of contact tracing apps
 - None has yet conducted efficiency and social impact assessment
 - Apps in most Member States had negligible impact (if any) on the spread of the pandemic, and, due to the low uptake, similarly negligible social impact
 - Member States should conduct research on why the technology and/or its implementations failed
 - Identifies several security gaps in many apps

¹P. Daniore et al., The SwissCovid Digital Proximity Tracing App after one year: Were expectations fulfilled?, Swiss Medical Weekly, Sep. 2021.

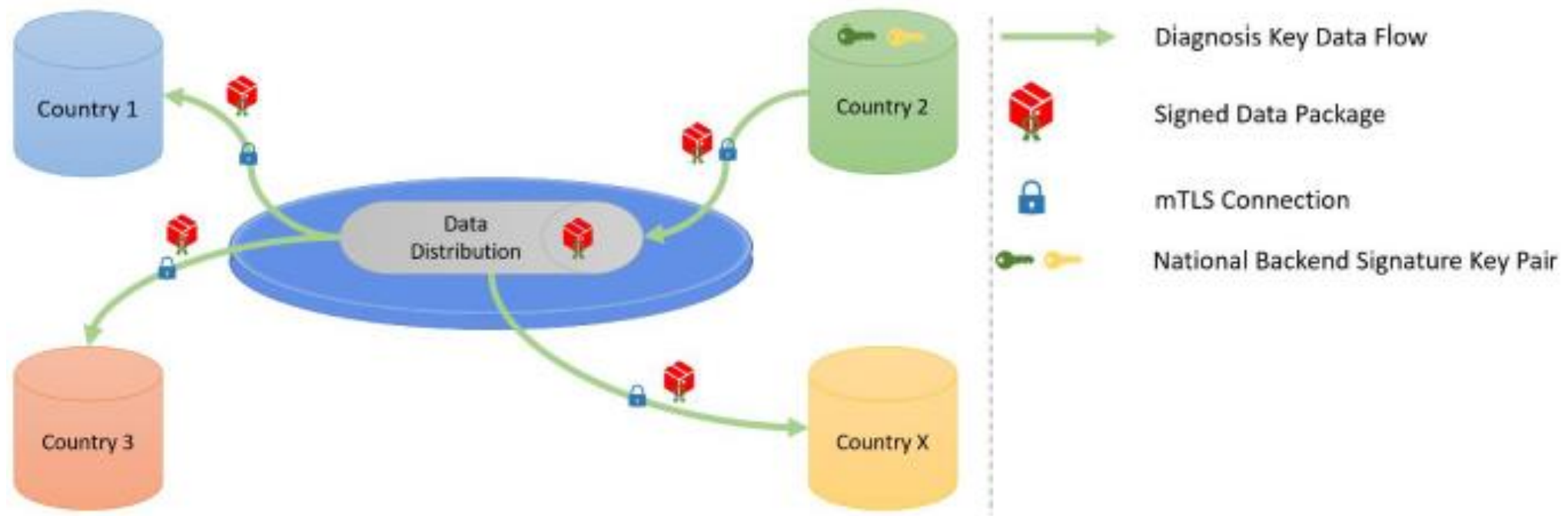
²Civil Liberties Union for Europe, Do EU Governments Continue To Operate Contact Tracing Apps Illegitimately?, Oct. 2021.

Security measures in place



- GAEN API
 - Only one country/state app approved by the local Public Health Authority
 - National infected keys validated by Google/Apple
 - Bluetooth identifiers change frequently and the payload is encrypted
- Infected user authenticates to upload keys via One-Time-Password (OTP)
 - OTP is appended to an SMS to prevent false positive claims
 - Multi-digit, expiry time, can be used only once
 - OTP submitted soon after the SMS → Prevents brute-force attacks

Secure communication with the EFGS



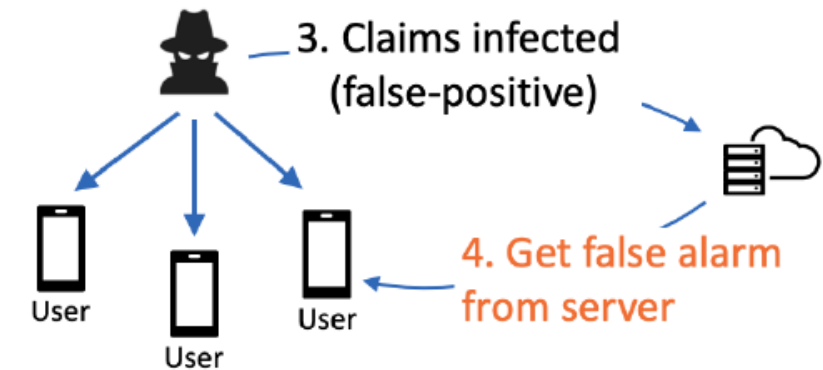
- Secure communication between the EFGS and the National Backends based on mutual Transport Layer Security (mTLS) authentication
- Each Member State has a private/public key pair that is used to provide data integrity by signing the batches of keys before uploading

Source: eHealth Network, European Proximity Tracing: An Interoperability Architecture for contact tracing and warning apps, Sep. 2020.

Known security flaws

- Analysis of 40 contact tracing apps for Android¹
 - Over **50%** of the apps pose potential security risks (one contained malware!)
 - **72.5%** employ cryptographic algorithms that are insecure or not best practice
 - False-positive claim
 - Attack addressed with OTP authentication. But what if OTP is shared/stolen/cracked?
- “advertising overflow” vulnerability [May 2021]²
 - Allows an attacker to interrupt the GAEN Bluetooth transmission with a malicious application installed on the same device
 - Any infected user who sends their data will not trigger any exposure warning

1. Broadcasts token



2. Record received token

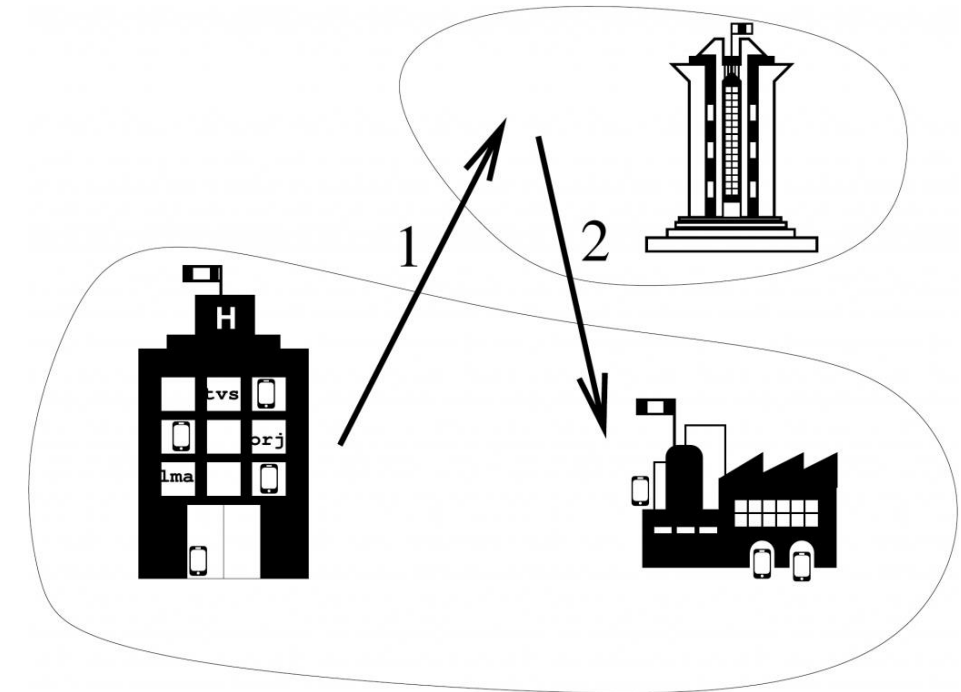
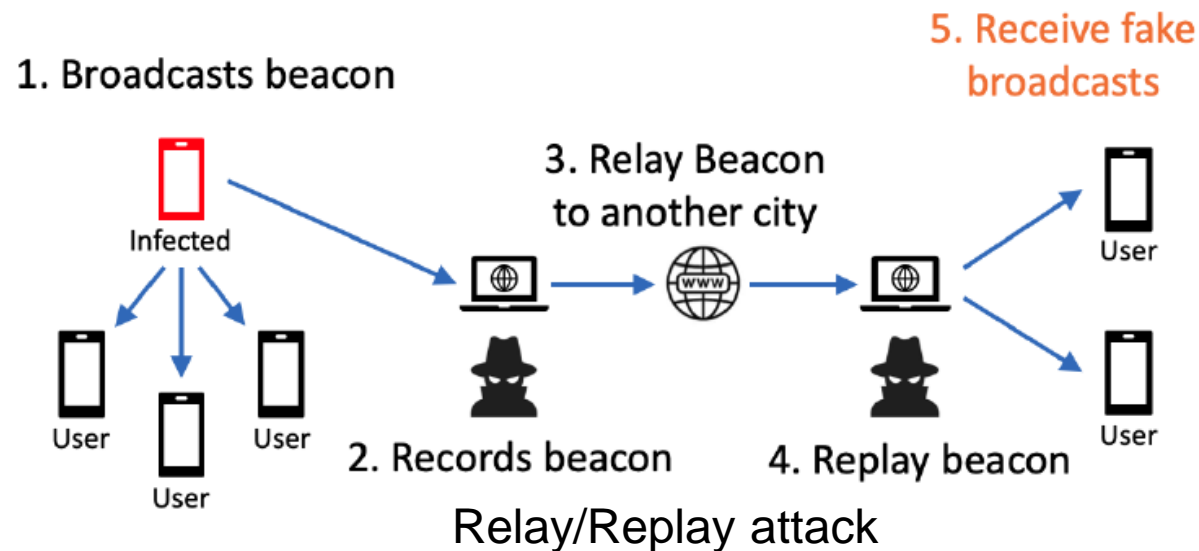
False-positive claim attack

¹R. Sun et al., An Empirical Assessment of Global COVID-19 Contact Tracing Applications, *43rd IEEE/ACM ICSE*, 2021.

²<https://algorithmwatch.org/en/tracers/portugal-cybersecurity-student-detects-bug-in-exposure-notification-apps/>

Potential security threats

- Relay/Replay attack^{1,2,3}
 - A centralized authority has more meta-information to detect such attacks
 - Could be partly mitigated in the decentralized case, but with significant complexity
 - The impact of the attack increases as more people run the tracing app
 - The attack can be targeted against key staff

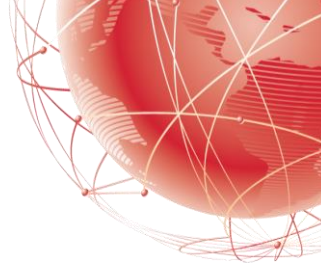


¹R. Sun et al., An Empirical Assessment of Global COVID-19 Contact Tracing Applications, *43rd IEEE/ACM ICSE*, 2021.

²Joel Reardon (AppCensus Blog), Proximity Tracing in an Ecosystem of Surveillance Capitalism, Dec. 2020.

³S. Farrell and D. Leith, A Coronavirus Contact Tracing App Replay Attack with Estimated Amplification Factors, Trinity College Dublin, May 2020.

What about privacy?



Is digital contact tracing an asset in the fight against pandemics or a privacy nightmare?

Image source: https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon

Privacy considerations



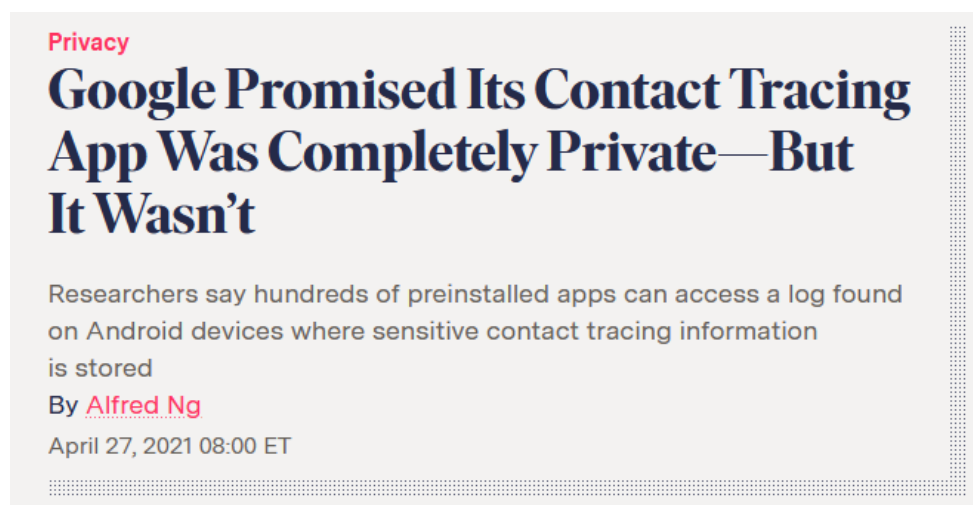
- Only used for exposure notification by public health authorities for COVID-19 pandemic management
- Bluetooth identifiers change every 10-20 minutes to prevent tracking
- The notified user does not know with *who*, *where*, or *when* the possible contact took place
- Not combined with location services (e.g., GPS, cellular, Wi-Fi) or other personal health data, e.g., EU Digital COVID Certificate
- Guidelines by the European Data Protection Board on the use of location data and contact tracing tools to comply with GDPR
- Several other data privacy arrangements approved by the national Personal Data Protection authority

Image source: Council of Europe, COVID-19 and Data Protection, Contact Tracing Apps

Known data privacy issues



- Data shared by GAEN-based apps¹
 - Health authority apps are generally well behaved from a privacy viewpoint
 - Users of such Android apps cannot avoid the use of Google Play Services
 - Google Play Services still contacts Google servers roughly every 20 minutes, potentially allowing fine-grained location tracking via IP address
 - [Personal] Data collection is enabled simply by enabling Google Play Services (e.g., phone IMEI, SIM serial number, phone number, WiFi MAC address, etc.)
- Potential vulnerability of the GAEN implementation reported by AppCensus²
 - GAEN logs crucial pieces of information to the system log, which can be read by hundreds of third-party apps
 - A bug fix was rolled out by Google



¹Source: Leith, D.J. and Farrell, S., Contact tracing app privacy: what data is shared by Europe's GAEN contact tracing apps, IEEE INFOCOM, 2021.

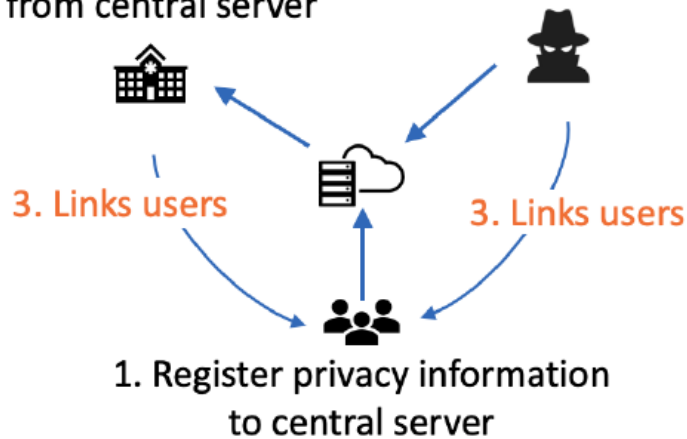
²AppCensus Blog, Why Google Should Stop Logging Contact-Tracing Data, Apr. 2021.

Known data privacy issues



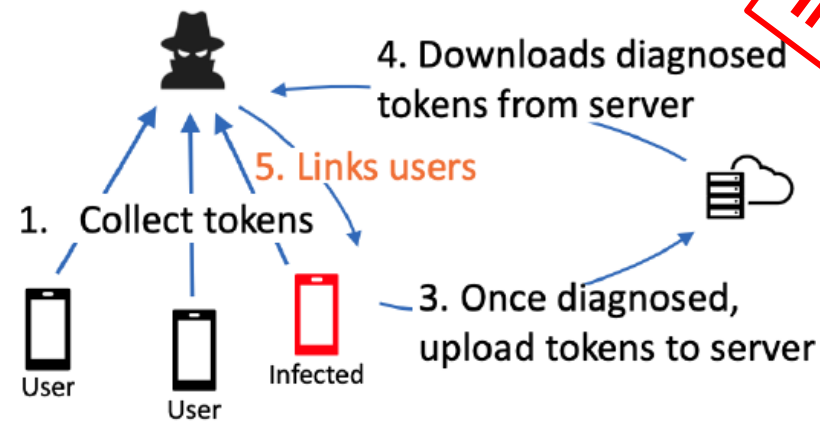
- Analysis of 40 COVID-19 contact tracing apps for Android¹
 - **55%** store sensitive information in clear text that could be read by attackers
 - Over **40%** of apps exhibit Manifest weaknesses, e.g., allowing permissions for backup (hence, the copying of potentially unencrypted application data)
 - Approximately **75%** of the apps contain at least one tracker that may expose personal data to third parties such as Facebook Analytics or Google Firebase

2. Obtains privacy data from central server 2. Attacks central server

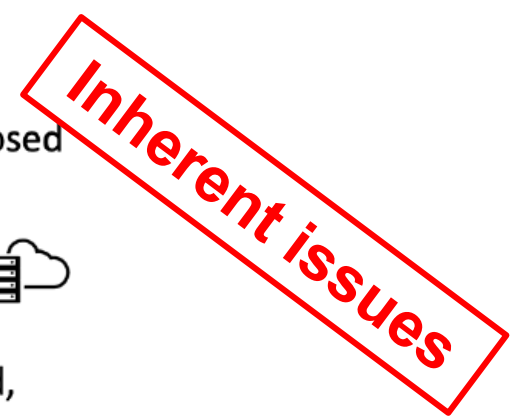


Linkage attack (centralized)

2. Logs additional information: day, time, duration, location ...

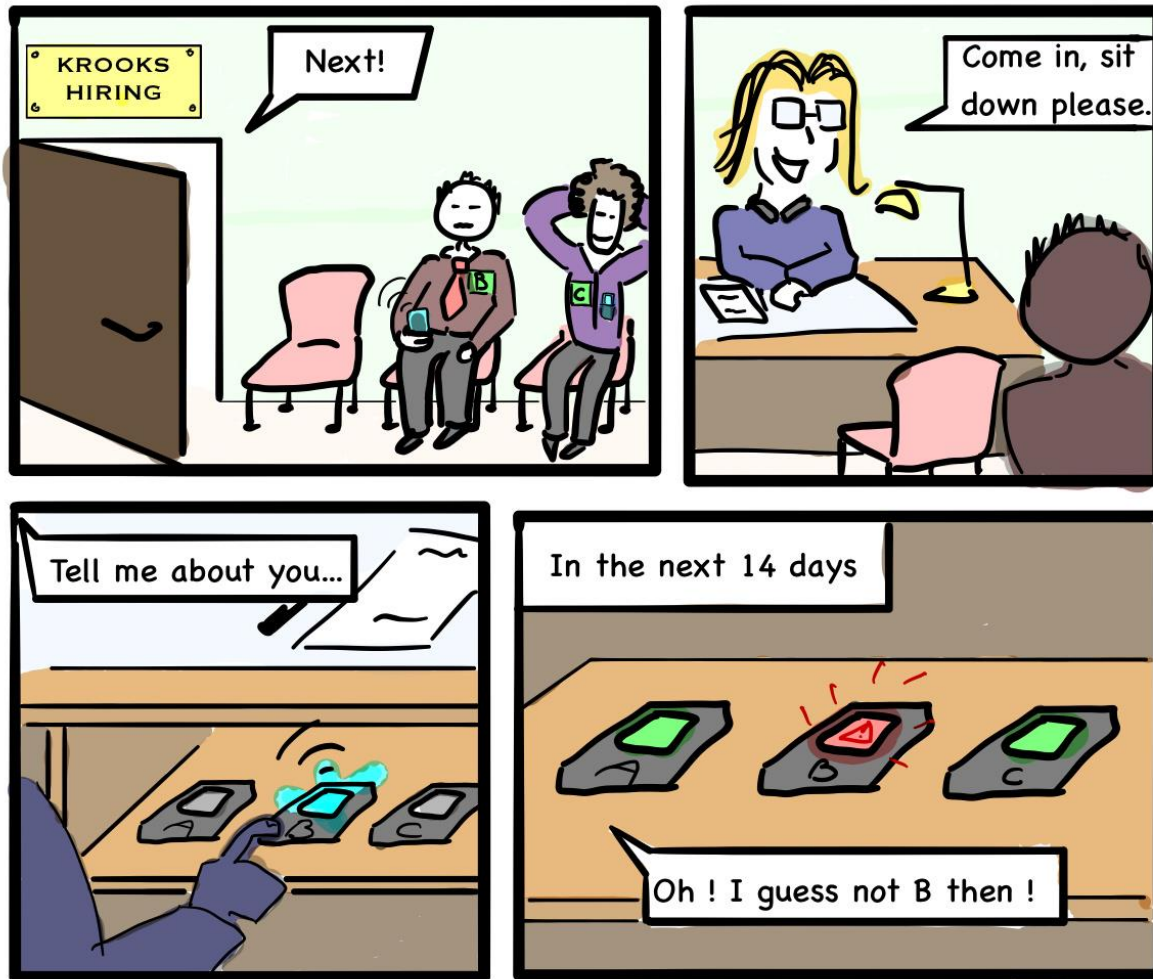


Linkage attack (decentralized)



¹R. Sun et al., An Empirical Assessment of Global COVID-19 Contact Tracing Applications, 43rd IEEE/ACM ICSE, 2021.

Privacy-preserving... or maybe not?



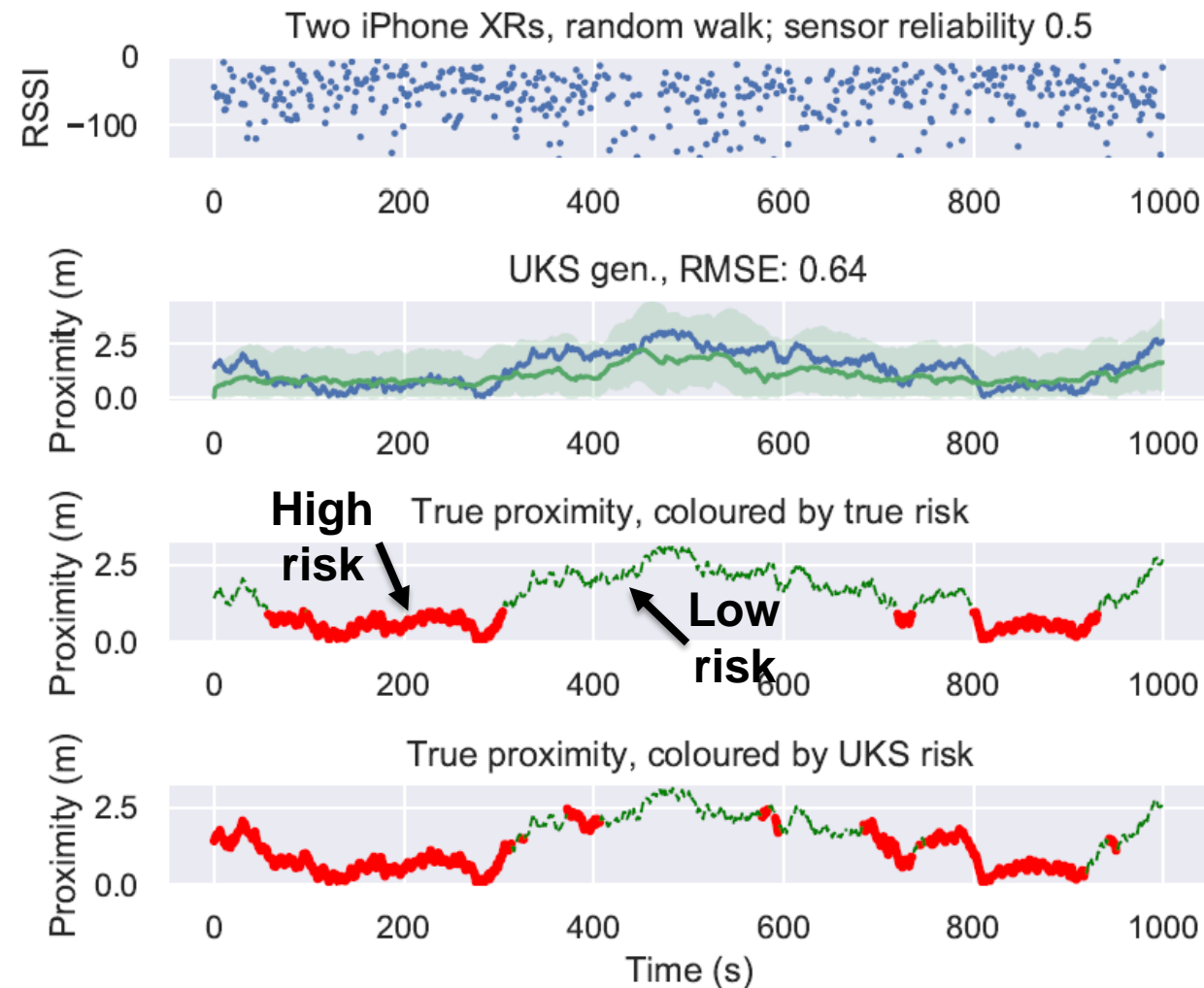
- More privacy issues regardless of the architecture, i.e., centralized or decentralized, and the implementation
- Specialists in cryptography, security or technology law warn that Bluetooth-based contact tracing is not harmless
- 15 scenarios illustrate various risks that are inherent to Bluetooth-based contact tracing

Source: Anonymous tracing, a dangerous oxymoron: A risk analysis for non-specialists, <https://tracing-risks.com/>

3.5G: Enhanced risk calculation



- Enhancements in the NHS COVID-19 app
 - Probabilistic risk score model¹
 - Unscented Kalman Smoother with generative observation model for inferring proximity from BLE RSSI readings²
- NIST's Too Close for Too Long (TC4TL) challenge
 - Estimate the distance and time between two phones given a series of RSSI values and other phone sensor data



¹Briers, M. et al., Risk scoring calculation for the current NHSx contact tracing app. *arXiv preprint arXiv:2005.11057*, 2020.

²Lovett, T. et al., Inferring proximity from Bluetooth low energy RSSI with unscented Kalman smoothers. *arXiv preprint arXiv:2007.05057*, 2020.

3.5G: Presence tracing

- The process of identifying the source of infection of the case under investigation, to identify further cases and contacts
 - A relatively small proportion of cases is responsible for a large proportion of transmission, e.g., in cluster or super-spreader events

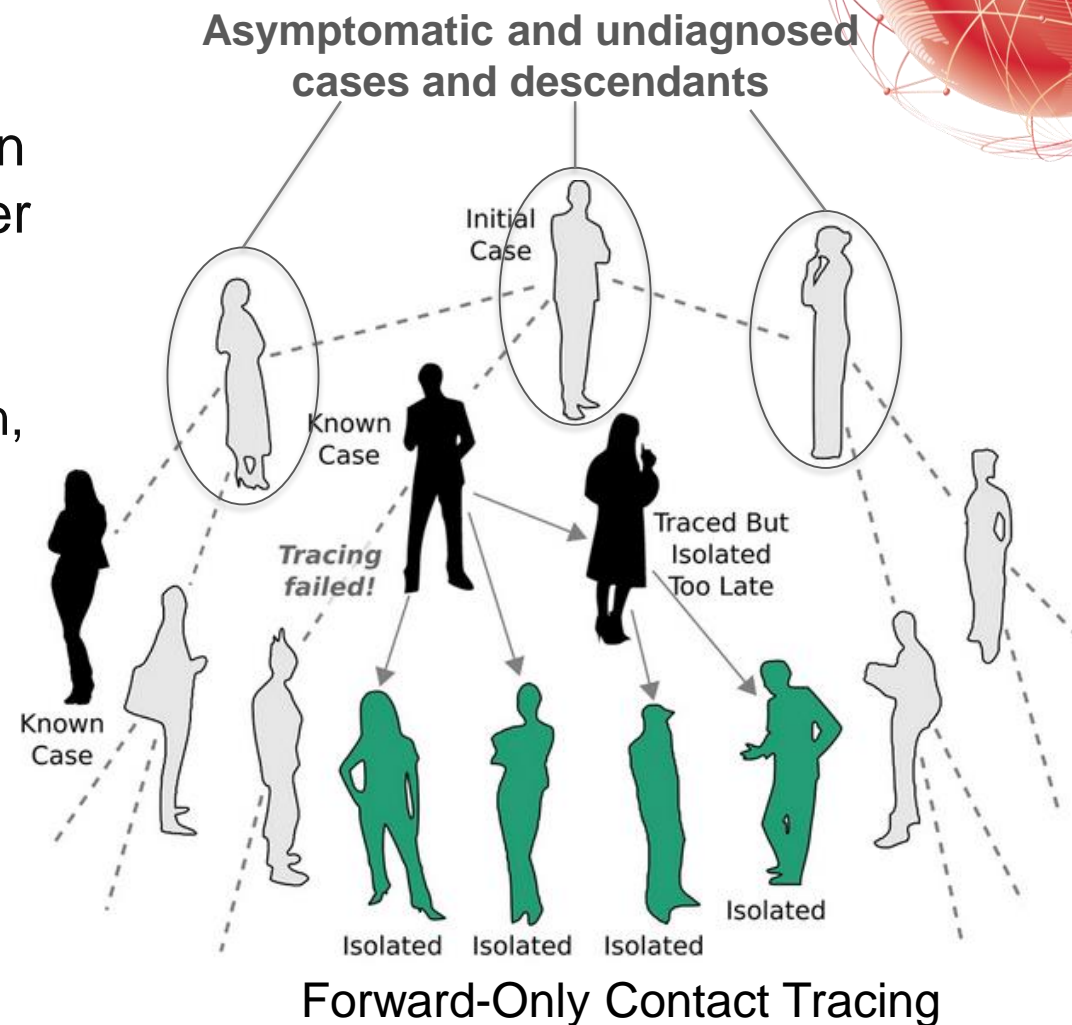
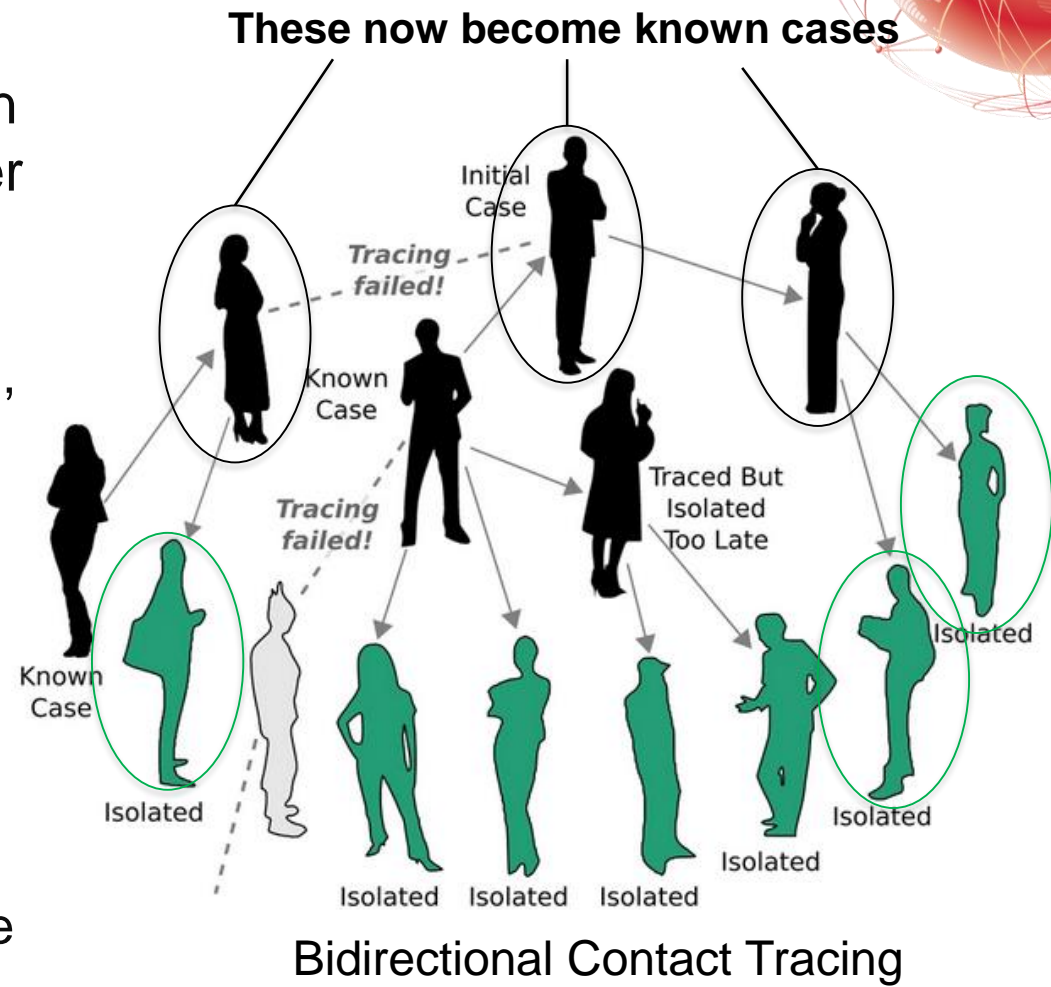


Image source: W.J. Bradshaw et al., Bidirectional contact tracing could dramatically improve COVID-19 control, Nature Communications, 2021.

3.5G: Presence tracing

- The process of identifying the source of infection of the case under investigation, to identify further cases and contacts
 - A relatively small proportion of cases is responsible for a large proportion of transmission, e.g., in cluster or super-spreader events
- Typically implemented with QR code scanning
 - *CrowdNotifier* Protocol + *NotifyMe* app (EPFL), *Cluster Exposure Verification (CLÉA) Protocol* (INRIA), *Event Registration* in CWA, ...
- How effective could it be?
 - Adding backward contact tracing could make ‘forward’ standard contact tracing **2-3 times** more effective in the UK context¹
 - Notifications for 226 risky venue events have been issued as of 20 Jan 2021. – NHS COVID-19 app



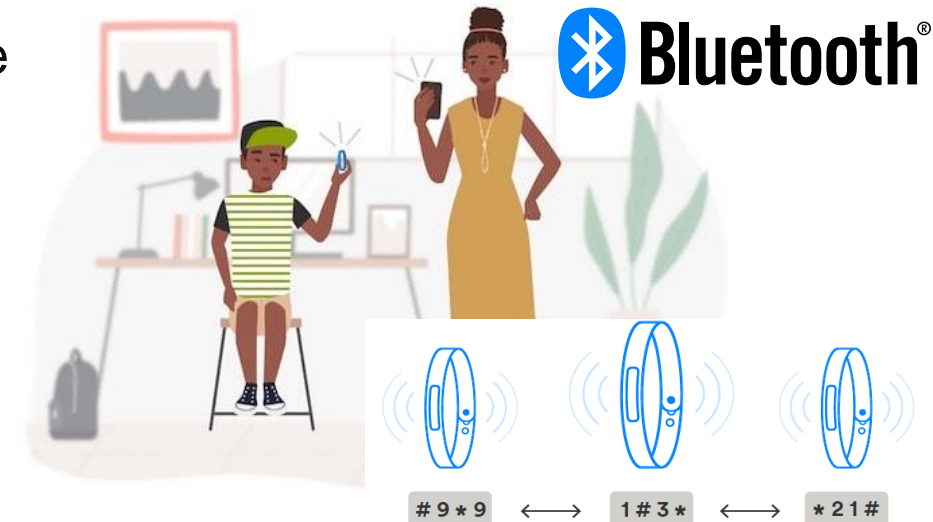
Bidirectional Contact Tracing

Image source: W.J. Bradshaw et al., Bidirectional contact tracing could dramatically improve COVID-19 control. *Nature Communications* 12, 232, 2021.

¹E. Akira et al., Implication of backward contact tracing in the presence of overdispersed transmission in COVID-19 outbreaks, *Wellcome open research*, Mar. 2021.

4G: Steps towards a global digital vaccine*

- BLE beacon-based notifications
 - TraceTogether Token, NIST Boulder device
- Bluetooth draft specification [2020]: Wearable Exposure Notification Service (WENS)
 - Will enable a non-Internet-connected wearable device to operate in a manner complementary with existing exposure notification apps
- Open source non-GAEN alternatives
 - Herald API provides proximity detection and data exchange between mobile phones, wearables, beacons and other devices.
 - OpenTrace Exposure Notification end-to-end system
- What about cross-continent interoperability of apps?
 - Global-scale federation service for infected keys



HERALD



*Term borrowed by D. Zeinalipour and C. Claramunt., COVID-19 Mobile Contact Tracing Apps (MCTA): A Digital Vaccine or a Privacy Demolition?, Panel @ IEEE MDM Conference, Jul. 2021.

4G: Steps towards a global digital vaccine



- Better proximity tracing = better risk computation → IPIN community to the rescue!
 - Indoor / outdoor classification → need to preserve privacy and be energy efficient
 - Sensors: GPS, RF, light, magnetometer, IMU → Typical accuracies 85%-95%
 - Accelerometer + gyroscope + light sensor: Accuracy 85% (outdoors) and 75% (indoors)¹
 - Transportation mode detection: walking, in vehicle, bicycle, bus, etc.
 - Activity detection: walking, running, stairs/elevator/escalator up & down, etc.
 - Carrying mode (handheld, bag, pocket) and phone direction (North, South, ...)
 - Wall/ceiling/glass separation: Ultrasound (through speaker & microphone)
- Other technologies: WiFi, Ultrasound, UWB, multi-sensor fingerprints
- Privacy-preserving localization (k-anonymity, l-diversity, t-closeness)
 - Temporal Vector Map² (k-anonymity Bloom filter), Paillier encryption³, Privacy-Preserving Indoor Localization (PPIL)⁴
 - Are existing location privacy-preserving mechanisms⁵ good enough for contact tracing?

¹M. Briers et al., Indoor/Outdoor Detection for Covid-19 Contact Tracing Apps, 2020.

²A. Konstantinidis et al., Privacy-preserving indoor localization on smartphones. IEEE Transactions on Knowledge and Data Engineering, 2015.

³Z. Yang and K. Järvinen, The Death and Rebirth of Privacy-Preserving WiFi Fingerprint Localization with Paillier Encryption, IEEE INFOCOM, 2018.

⁴K. Järvinen et al., PILOT: Practical Privacy-Preserving Indoor Localization Using Outsourcing, IEEE EuroS&P, 2019.

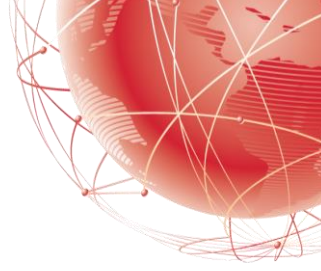
⁵S. Oya et al., Rethinking Location Privacy for Unknown Mobility Behaviors, IEEE EuroS&P, 2019.

Take home messages



- A long way to go from a “nice to have” to “a need to have” app
- The technology was put out in the field too early
 - Use COVID-19 pandemic as a testbed for improving the technology
- Used as a supplement to manual contact tracing, tracing apps can become instrumental to curb this and future pandemics
 - Even after vaccines it is worth investing to contact tracing technology
- A global multi-cultural citizen project
 - The mechanics are equally important to the user-perceived efficacy
- Addressing privacy concerns for mass surveillance is crucial for the voluntary use and uptake of tracing apps
 - Should the technology belong to tech companies or governments?

Extra Slides



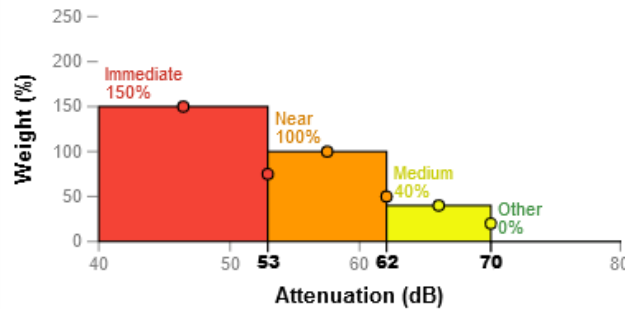
COVID19 Risk Score Tuner – Narrower Net



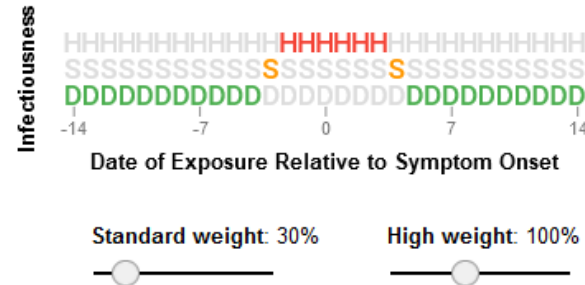
Exposure Notification Parameters

Preset Configurations: LFPH-Narrow No file selected.

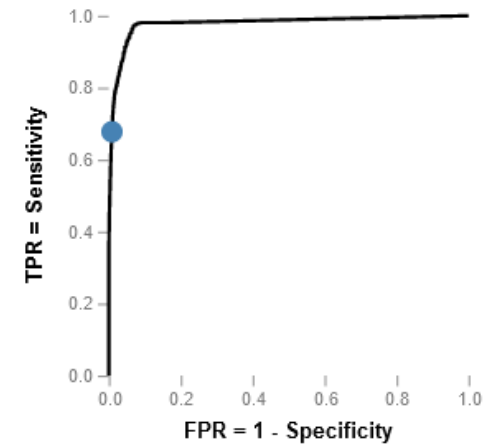
Bluetooth Attenuation Settings



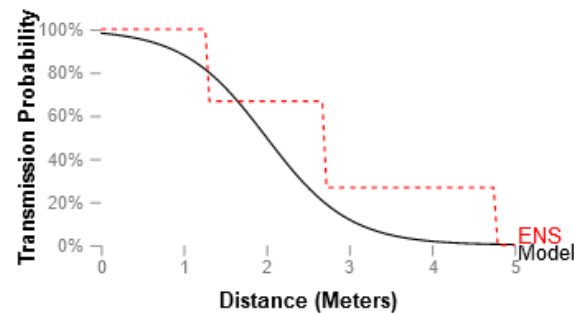
Symptom Onset Settings



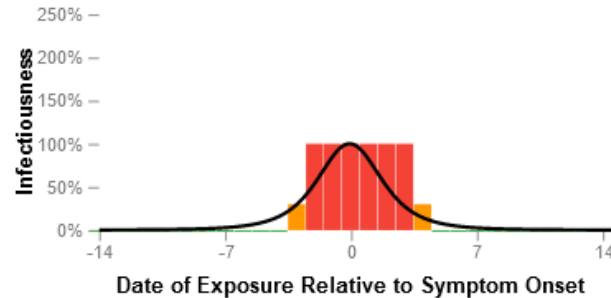
AUC: 0.98 [0.97 - 0.98]



Transmission v. Distance



Infectiousness v. Time



Risk Threshold: 15 min

Alerts: 0.10 [0.08 - 0.11]
 Specificity: 0.99 [0.99 - 0.99]
 Sensitivity (Recall): 0.68 [0.64 - 0.72]
 PPV (Precision): 0.91 [0.90 - 0.93]
 NPV: 0.96 [0.95 - 0.96]

Simulation Parameters

Evaluation Metric Parameters

Source: Murphy, K., Kumar, A. and Serghiou, S., 2021. Risk score learning for COVID-19 contact tracing apps. arXiv preprint arXiv:2104.08415.
<https://risk-score-tuner.appspot.com/>