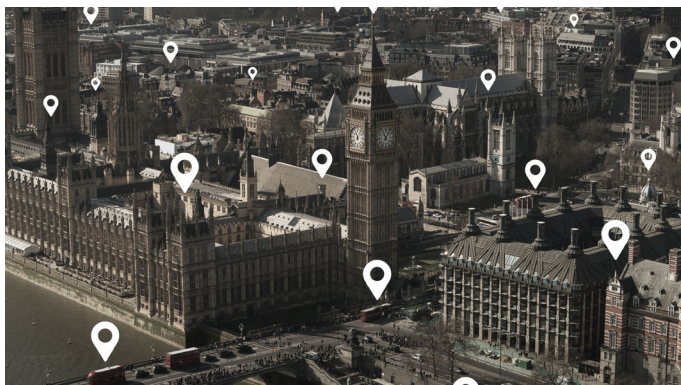


COVID-19: The Internet of Things and Cybersecurity

Prepared by Fredrik Skippervold and Dr Catherine Wheller



The COVID-19 pandemic has inspired a range of Internet of Things (IoT) innovations to help stop the spread of the virus. A key to tackling the spread is the [identification and quarantine of infected individuals](#)¹. This process requires accurate, and almost real-time information about the locations and people an infected person has interacted with. Using mobile phone locations for contact tracing is therefore proving a popular strategy for many governments to tackle the outbreak. However, if privacy concerns cause users to avoid these measures then they will not be effective.

How a conventional mobile phone contact tracing app works

A contact tracing application on a mobile phone collects data on the proximity and infection status of contacts. An infected user can upload their data, which has been collected using either Bluetooth signals or GPS location, to the relevant authority. Other users who interacted with the infected person, can now be informed that they are at risk.

Notable examples around the world

China

China has implemented an [application](#)² which assigns colour codes to users based on their health status and travel history, and a QR code that can be scanned by authorities; Green = travel freely; Yellow = self-isolation; Red = confirmed case, quarantine.

Overview

- A growing number of countries are testing mobile phone contact tracing applications to combat the spread of COVID-19.
- This technology utilises mobile phones by tracing individuals' location data or interactions via Bluetooth.
- There are concerns regarding the privacy and security of user data when using these apps.
- Privacy concerns may stop the uptake of contact tracing apps in the UK
- Solutions are being developed to maintain user privacy from outsiders, contacts and authorities.
- Smart wearables are being developed to aid contact tracing and it is important for these to be developed with privacy at the core of their design.

These measures have stopped those who pose a risk of infection from travelling. This has slowed the rate of coronavirus in the country. There are, however, [reports](#)³ of this system not being transparent and it risking the privacy of individuals.

South Korea

South Korea launched a central tracking app – [Corona 100m](#)⁴, which publicly informs citizens of known cases within 100m of their location. Text messages containing personal information about diagnosed carriers are sent to inform citizens. South Korea has largely been successful in stopping the spread of the virus. Concerns have been raised about the personal nature of the data [fuelling social stigma](#)⁵.

Singapore

Singapore updates a map with detailed information about each COVID-19 case. The [TraceTogether](#)⁶ app uses Bluetooth signals to determine when your phone is near another phone with the app installed. The phones then exchange anonymised IDs, which

are stored in encrypted form on these phone only. If a user gets infected, they will be asked to give authorities access to the TraceTogether data. No geolocation or personal data is collected. Clear terms and conditions are published in their [privacy statement](#)⁷.

TraceTogether provides security between users, but relies on the assumption that the government is honest and trusted. A [review by researchers at The Alan Turing Institute](#) concludes that TraceTogether provides a strong baseline of privacy, however it is unlikely that solutions of this nature will be widely adopted in the UK due to differing cultural views regarding the power the government should be afforded.⁸

What is the UK doing?

NHSX together with the University of Oxford have been working on a contact tracing app. There is a big emphasis on preserving individual privacy and this may have delayed its deployment. It has been [reported](#) that such an app would enable a week's worth of manual detective work to be done in an instant.⁹ The study by the team at the University of Oxford's Big Data Institute and Nuffield Department of Medicine was [published](#)¹⁰ in the journal Science.

UK and EU researchers are developing privacy-preserving contact tracing protocols – see below.

A cautious approach is necessary when evaluating the effectiveness of this technology in other countries

Although South Korea has been successful in slowing the spread of coronavirus, the mobile-phone contact tracing app cannot claim all the credit. As well as using a GPS phone tracking app, the [government check credit card records and surveillance video](#)¹¹. There are also websites and smartphone apps that detail, “sometimes minute-by-minute, the timelines of infected people’s travel – which buses they took, when and where they got off, even whether they were wearing masks”¹².

Negative consequences of an app approach

[The New Humanitarian](#)¹³ have listed areas where such an app may have negative consequences:

- Individual risk estimations may lead people to seek more testing than otherwise – which may contribute to overwhelming the health

Which countries are using this technology?

According to [GDPR Hub](#)²⁸, the following regions are using contact tracing apps or frameworks:

(Mainly) Decentralised contact tracing apps or frameworks

- Pan-European: Framework for Contact Tracing (PEPP-PT)
- Pan-European: Decentralised Privacy-Preserving Proximity Tracing (DP-3T)
- Austria: “Stopp Corona” app (Red Cross)
- Austria: NOVID20 (Private)
- Finland: Ketju project (Private & Public)
- Germany: “GeoHealthApp” (Private)
- Iceland: Government app project
- Ireland: HSE App (Government)
- Israel: “Hamagen” app (Government)
- Italy: Rilevatore terremoto
- Italy: Various other apps
- Norway: App by the Institute of Public Health
- Singapore: “TraceTogether” app (Government)
- Switzerland: “WeTrace” app (Private)
- United Kingdom: NHSX/University of Oxford tracking app (Government)
- United States: Covid Watch (Stanford University)
- United States: CoEpi

Centralised contact tracing systems

- Czech Republic: Multi-Source Contact Tracing
- Slovakia: Multi-Source Contact Tracing
- Israel: Use of Mobile Network Data
- South Korea: Multi-Source Contact Tracing

system.

- Only half the world’s population have smartphones. This approach is likely to miss the most vulnerable groups.
- Concern that the government will hold onto the new surveillance powers once the pandemic is over.

Calls for privacy at the heart of design

An [open letter](#) was published on March 21st urging the NHSX to follow “ethical best practices” in designing contact tracing apps. The letter calls for:

- Working in the open to build trust and minimise speculation,
- Introducing emergency governance measures,
- Balancing the needs of individuals and the benefit to society.

One app or many?

The EU Data Protection Supervisor has [recommended](#)¹⁴ that a single European contact tracing app be used to tackle the pandemic.

Several initiatives have emerged:

Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)

[PEPP-PT](#)¹⁵ enables tracing of infection chains across national borders. “If someone travels from [one European country to another](#), they can still receive or trigger an alert, even if using a different app to locals”¹⁶.

Positively, one of the project’s coordinators, Chris Boos, has said that “about 90% of the work has already been done and the [technology should be ready for release](#) (this week)”¹⁷.

The app would [use Bluetooth and all data will be encrypted and stored on the user’s device](#). If a user becomes infected, they can be sent a one-time code that allows sharing of their proximity history¹⁸.

The German Chancellor, Angela Merkel, [says](#)¹⁹ she would use this app on her personal devices.

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

The [TCN Coalition](#)²⁰ was formed on April 5 as a group for privacy-first digital contact tracing protocols to fight COVID-19. A global community of technologists, privacy experts, and epidemiologists has worked towards a secure, privacy-first, GDPR-compliant, and open-source approach to enable globally compatible digital contact tracing.

European privacy experts have [proposed a decentralised system for Bluetooth-based COVID-19 contacts tracing](#)²¹ which they argue offers greater protection against abuse and misuse of people’s data than apps which pull data into centralised pots. The proposed protocol is called [DP-3T](#)²². They urge all major technology companies, app developers and governments to implement apps compatible with this shared protocol.

[Simplified Three page brief](#)²³

[Full White Paper](#)²⁴

TraceSecure: The Alan Turing Institute

The Alan Turing Institute has [proposed privacy preserving solutions building on the TraceTogether app in Singapore](#).²⁵ Its lightweight nature and strong privacy properties mean that the additional methods they propose could be of use in combating the spread of the virus worldwide.

DP-3T is decentralised, which means there is no central collection of potentially sensitive user information. In contrast the Turing protocol provides the government with a pseudonymised version of interactions. This requires a greater level of trust in the government. However, DP-3T has the downside that a list of infected users’ broadcasts is made public.

The researchers note that DP-3T is a strong proposal for privacy preserving contact tracing however differs in what attacks are acceptable.

Combining contact tracing apps with IoT smart devices

Hong Kong’s Electronic Wristbands

From March 19 Hong Kong’s government [enforced the use of an electronic wristband](#)²⁶, accompanied by a smartphone app, for all arriving passengers in an effort to enforce the self-quarantine measures. This electronic bracelet made sure people were self-quarantining properly by requiring everyone to walk around the corners of their home to precisely track the coordinates of the living space. The wristbands were [supplied by Logistics & Supply Chain MultiTech R&D Centre](#)²⁷, and are waterproof.

Endnotes

- 1 **<https://science.sciencemag.org/content/early/2020/03/30/science.abb6936>**
- 2 <https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>
- 3 <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>
- 4 <http://www.koreaherald.com/view.php?ud=20200311000132>
- 5 <https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives>
- 6 **<https://www.tracetgether.gov.sg>**
- 7 <https://www.tracetgether.gov.sg/common/privacystatement>
- 8 **<https://arxiv.org/pdf/2004.04059.pdf>**
- 9 <https://www.bbc.co.uk/news/technology-52095331>
- 10 <https://science.sciencemag.org/content/early/2020/03/30/science.abb6936>
- 11 https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html
- 12 <https://www.nytimes.com/2020/03/23/world/asia/coronavirus-south-korea-flatten-curve.html>
- 13 <https://www.thenewhumanitarian.org/opinion/2020/03/30/coronavirus-apps-technology>
- 14 <https://www.bbc.co.uk/news/technology-52189551>
- 15 **<https://www.pepp-pt.org>**
- 16 <https://www.bbc.co.uk/news/technology-52121264>
- 17 <https://www.bbc.co.uk/news/technology-52121264>
- 18 https://www.theregister.co.uk/2020/04/06/pan_european_privacy_preserving_proximity_tracing_plan/
- 19 https://www.theregister.co.uk/2020/04/06/pan_european_privacy_preserving_proximity_tracing_plan/
- 20 <https://tcn-coalition.org/>
- 21 <https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/amp/?guccounter=1>
- 22 **<https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf>**
- 23 **<https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Simplified%20Three%20Page%20Brief.pdf>**
- 24 <https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf>
- 25 <https://arxiv.org/pdf/2004.04059.pdf>
- 26 <https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html>
- 27 https://www.news.gov.hk/eng/2020/03/20200316/20200316_202554_111.html
- 28 https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

Key references in bold.