PETRAS

LANDSCAPE BRIEFING

NUMBER 03 | 28 APRIL 2020

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. This is the third edition of COVID-19: IoT and Cybersecurity and builds on the rapid advances in the issues surrounding digital contact tracing applications and smart devices in the UK and beyond.

Past editions are found here.

Overview

- The UK Government has announced their approach to contact tracing will involve an app in conjunction with manual contact tracing.
- The privacy community is calling for the NHSX to release the source code before the app is released.
- In addition, the limitations of a digital solution must be acknowledged.
- Legal protections are still being updated, with the Coronavirus (Safeguards) Bill 2020 receiving positive attention globally.
- The debate on centralised and decentralised apps is ongoing, with most of Europe moving towards decentralised versions.
- The WHO urges caution towards immunity passports, as the evidence for immunity is not settled. However, some countries are going ahead with these plans.
- Smart devices are also being supported by government and private industry to maintain quarantine, check and report symptoms and guarantee social distancing.

Integrating digital and manual contact tracing in the UK

The UK Government has announced a two-pronged approach to track, trace and isolate new cases of coronavirus in order to start lifting lockdown restrictions. The approach requires resuming manual contact tracing by Public Health England by deploying 18,000 human contact tracers[1], as well as developing a smartphone app to automatically alert people who may have come into contact with an infected person.[2]

The app is being tested at an RAF base, with estimations of a mid-May public release.[3]

Matthew Gould, CEO of NHSX has released details of the NHSX app[4] and makes it known that they have not let 'urgency compromise our commitment to transparency, ethics and the law'. The statement confirms that NHSX will publish the key security and privacy designs alongside the source code so privacy experts can provide comment. An NHSX Ethics Advisory Board provides independent advice and recommendations for a contract tracing app to control the spread and minimise the effects of COVID-19.[5]

Developers are called to be candid about the limitations and implications of digital contact tracing

There have been cautions raised about placing too heavy a reliance on digital contact tracing. In a policy note to the Scottish Government, the director of the Newcastle University Centre for Excellence in Regulatory Science puts forward that localised approaches to contact tracing involving local public health teams working with local authorities on local COVID surveillance is the key to stopping transmission.[6]

Box 1: Questions to determine the extent to which a contact tracing app is ethically justifiable

Is the correct system being developed?

- Is it a necessary solution?
- Is it a proportionate solution?
- Is it scientifically sound?
- Is it temporary?

Is the system being developed correctly?

- Is it voluntary?
- Does it require consent?
- Are the data kept private and users' anonymity preserved?
- Can the data be erased by the users'?
- Is the purpose defined?
- Is it only used for prevention?
- Is it used to monitor users' behaviour?
- Is it open-source?
- Is it equally available?
- Is it equally accessible?
- Is there an end life process to retire the system?

See full paper for sub-questions

In a US context, some researchers with expertise in technology, law and policy, and epidemiology have written about their concern for automated technology in infection control, with the worry that contact tracing apps could serve as 'vehicles for abuse and disinformation'. They believe that apps that 'notify participants of disclosure could...help direct testing resources to those at higher risk' and that 'anything else strikes us as implausible at best, and dangerous at worst'.[7]

While assurances are welcome, the digital privacy community are calling for more open conversation and transparency before the app is released

Yesterday, 27 April, NHSX confirmed that they will not be using the contact tracing model proposed by Apple and Google. Instead, the NHSX app will be a centralised model.

Without compliance with the Apple system which will allow the app to run in the background while exchanging Bluetooth signals, the NHSX app will require the phone to 'wake up' each time a signal is shared. This is a more energy intensive operation and results in power consumption problems on iPhones.[8]

Nevertheless, with efforts from GCHQ's National Cyber Security Centre and NCSC, the NHS said 'it has a way to make the software work 'sufficiently well' on iPhones without users having to keep it active and on-screen'.[9]

The Open Rights Group postulate that the governments proceeding with centralised apps, such as France, Germany and the UK are hoping that Apple and Google will eventually allow them to access the new API. The group further states that a centralised app may have clinical reasons for adoption, however this needs to be an open conversation.[10] The NHSX believes a centralised system will give it more insight into Covid-19's spread.

Researchers from the Oxford Internet Institute and the Alan Turing Institute have produced an inclusive framework comprising 12 factors to guide the design and development of ethical digital tracing systems. The framework is summarised in Box 1. The paper highlights the need to constantly evaluate the use of contact tracing apps throughout the progression of the pandemic, as scientific and ethical justifications change. The paper warns governments to not release apps which have not had scrutiny on their design and ethical justification, and that 'governments have one chance to get an intervention right, as repeated failures and overly high costs breach citizens' trust'.[11]

Discussion on appropriate legal provisions to ensure public trust in the uptake of contact tracing is continuing

The Coronavirus (Safeguards) Bill 2020 has been updated on 21 April (Version 3). The model statute provides safeguards in relation to the symptom tracking and contact tracing apps that are being rolled out in the UK. On 28 April, a formal meeting of the Science and Technology Committee heard oral evidence on essential minimum safeguards on how tech can be used to ease lockdown.[12]

Addressing the 'digital divide' and the inequality of accessibility

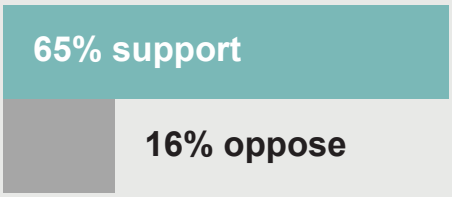
There is a risk that many of those most at risk will not benefit from the new technology.

PETRAS is funded by the UKRI via the Security of Digital Technologies at the Periphery (SDTaP) programme.

A survey Ipsos Mori, commissioned by the FT, found that two-thirds of Britons are in favour of government phone tracking to help tackle the pandemic.[48]

How strongly, if at all, would you support or oppose mobile phone service providers giving the Government people's mobile phone roaming data for each of the following reasons?

'So the government can track people who have been diagnosed with the Coronavirus, and those they have come into close contact with, so they can advise those individuals to self-isolate themselves'



There is still concern as to whether or not the uptake of the NHS app once launched will be sufficient. 12% of smartphones in active use in the UK do not support the Bluetooth LE standard required. The BBC has reported that the use of low-cost wearable Bluetooth devices by those without a compatible handset is under consideration.

Work is ongoing on an interoperable approach to contact tracing within Europe

The European Data Protection Board (EDPB) adopted Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak on 21 April. The guidelines recommend a common European approach, or an interoperable framework, and acknowledge that GDPR and 'ePrivacy Directive' of 2002 contain the relevant rules for data collection in a pandemic. Because of this, the EDPB has taken the position that contact tracing should be voluntary and focus on proximity information rather than tracing movement.

One of the debates is whether the contact tracing system is centralised, where health authorities/ government manage the data, or decentralised, where greater control of the data is with the users. The EDPB suggests 'both should be considered viable options, provided that adequate security measures are in place'. The recommendations do note that decentralisation is more in line with the data minimisation principle.[13]

A rapid review of evidence on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis

The last issue of the landscape briefing linked to The Ada Lovelace Institute's rapid evidence review[44] on the technical and social considerations of using technology to transition from the COVID-19 crisis. The review concludes that rushed deployment of technical solutions without evidence and independent oversight may undermine public trust and impede effectiveness.

They have since published short summaries for three audiences:

- Government and policymakers[45]
- Parliament[46]
- Technology providers and developers[47]

More European countries are moving towards decentralisation, however some are sticking with a centralised solution

A notable change in recent days is that Germany has changed course to back an the Apple and Google contact tracing approach, joining several other European countries in adopting privacy-preserving decentralised protocols.[14] Estonia[15], Austria[16], and Switzerland[17] have all confirmed they are proceeding with developing apps using either the Google and Apple protocol, or the privacy-preserving DP-3T protocol.

This leaves France as an outlier. As it stands, France does not want to build in the privacy measures required by Google and Apple and has been pressing the tech companies to alter their requirements.[18]

On 18 April, the French Institute for Research in Computer Science and Automation (Inria) and Fraunhofer Institute for Applied and Integrated Security (AISEC) proposed ROBERT (robust and privacy-preserving proximity tracing protocol) as a contact tracing system. However, in an analysis of ROBERT by the DP3T team several design issues are raised, and the team conclude that 'adopting this system would open up significant avenues for systemic misuse and that it does not sufficiently prevent function creep or engender the trust that is crucial for public adoption, safety and legitimacy'.[19]

Hundreds of France's security experts have signed an open letter calling on the government to reconsider the centralised approach. Many of these signatories state they work for Inria. Researchers at Inria have also published a risk analysis on contact tracing apps, including the ROBERT proposal.[20]

Australia has launched a centralised app, however it does come with some legal protections

The Australian Government released a contact tracing app on 26 April called COVIDSafe. It is based on a centralised model where 'encrypted contact information from the app will be uploaded to a highly secure information storage system once an infected user consents to the upload'. At the end of the pandemic, users will be prompted to delete the COVIDSafe app from their phone.[21]

As it stands, the app can run in the background on Android phones, however will face limitations on iPhones when at low battery.[22]

The Australian Minister for Health has set out a Determination under the Biosecurity Act to protect people's privacy and restrict access to app information to state or territory health officials for contact tracing purposes only.[23] The Government is proposing to introduce the legislation to Parliament in mid-May to enshrine the principles into law.[24] A Privacy Impact Statement (PIA) [25] for the app was also released. The belated release of the PIA, as well as the lack of open source code before public release has also been criticised.[26]

The Australian Law Council released a statement saying that privacy concerns still exist, namely that the Determination makes no provision for oversight and reporting on its use. However, they welcome the 'voluntary opt-in nature of the app, the prohibition of the collection, use and disclosure of COVID-19 app data for anything other than the primary purposes of the tracing app, and the explicit prohibition on the coercive use of the app as a condition of employment (current or former), entry to premises or participation in activities.'[27]

Restoring a sense of normalcy with immunity passports is tempting, however the science supporting their effectiveness isn't there yet

In a report published by the Tony Blair Institute for Global Change on 24 April, the creation and use of a digital credential is explored as a method to help lift lockdown restrictions in situations where people have had the virus and are now presumed immune, and for significantly lower risk demographics. They propose that this digital credential be stored on the person's smartphone.[28]

On the same day, the World Health Organisation (WHO) published a scientific brief on these immunity passports that would enable people to travel or to return to work assuming that they are protected against re-infection. The WHO stated that 'there is currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection'. In fact, the WHO considers that the creation of these 'immunity passports' and 'virus-free' certificates, may increase the risk of continued transmission as 'people who assume that they are immune to a second infection, because they have received a positive test result, may ignore public health advice'.[29]

Despite these warnings, two days later on 26 April, Chile announced its plans to continue their 'virus-free' certificate project.[30] These certificates would be handed to those who have recovered from COVID-19 which would allow them to return to work. Chile's Deputy Health Minister has said that the purpose of these certificates are not to evidence someone's immunity, rather, to show that these people have completed the self-isolation process and therefore have a lower probability of contracting the disease again.[31]

There are ethical concerns to take into account, especially if voluntary technologies edge towards being compulsory for social participation

If prior infection does provide sufficient immunity, and passports begin to be rolled out, then there is the potential for them to be used to discriminate against untested people and those who aren't immune.[32] Protections need to be in place to protect communities that can be harmed by the collection and potential exploitation of this data.

To address this in the UK, the draft model statute Coronavirus (Safeguards) Bill 2020 (see further above) sets out to introduce 'coronavirus status' as a protected characteristic under the Equality Act 2010.[33]

The Belgian government's Risk Assessment Group and Scientific Committee on the Coronavirus,

strongly oppose the idea of immunity passports. A member of the committee believes this would 'lead to forgeries', and in turn, 'lead to people wilfully infecting themselves to the virus'.[34]

Smart devices are also being used to maintain quarantine, check and report symptoms, and guarantee social distancing

United Kingdom

A wearable patch has been developed and trialled in partnership with the NHS in northwest London. The sensor is used to remotely detect signs that a patient's condition is worsening, and detects vital signs every two minutes, in contrast to manual recording hours apart. The trial is testing whether remote detection can benefit patients and staff in quarantine facilities by enabling clinical monitoring while keeping physical distance to minimise the spread of coronavirus.[35]

Bulgaria

Private industry are providing fifty 'LifeWristbands' to the Regional Health Inspectorate in Sofia, Bulgaria. The devices will be distributed to people quarantining at home, and this pilot stage is scheduled to last three months. The users health will be continuously monitored and their location tracked using a GPS module. This will help the Regional Health Inspectorate see if users are in their homes. The LifeWristbands are equipped with a SIM card which will allow law enforcers to call in and check whether quarantined individuals are at home. This function will reduce the risk of infection of officers and lower operating costs for the agencies.[36]

Liechtenstein

As part of the COVI-GAPP study[37] and supported by the Liechtenstein Government, sensory bracelets are being given on a voluntary basis to approximately 2000 inhabitants (roughly five percent of Liechtenstein's population). The devices monitor skin temperature, resting pulse rate, perfusion, breathing rate and heart rate variability. The purpose is to collect data that will hopefully allow early detection of Covid-19 as well as becoming a remote measuring device for high-risk groups that are self-isolating. The researchers hope that first round results will support expansion before the potential second wave of infection.[38]

Belgium

In a response to the call by the Flemish Government to create digital solutions for helping society through the current corona crisis, a private company has launched a digital bracelet to prevent coronavirus infections on the workfloor.[39] They claim that the bracelet will make it safer for employees to resume work. The bracelet works by sending warning signals (visual and vibration) to the user when they get too close to another worker. Location data will not be shared with the employer. The bracelet also permits contact tracing within the workplace, so an infected user can consent to a health advisor accessing a list of wearable IDs that have a logged contact-event.[40]

Private industry are moving forward with apps to aid social-distancing at the office, but they may not be voluntary

While the issue of immunity passports is controversial, the danger of sending people back to work at their offices may be somewhat relieved with the development of new office monitoring apps. However, these may not come with privacy guarantees.

In a US context, PwC have said companies could make these apps mandatory, ensuring that the necessary adoption levels are reached.[41] One company, is building a tool designed to track where people have been to within a few centimetres [42] in order to scrub down locations where an infected person has been. Another company has proposed 'Universal Contact Tracing', and is moving away from smartphones, recognising that many vulnerable people would be left out and that certain facilities such as hospitals or construction sites may prohibit phone use. Instead, Universal Contact Tracing uses simple Bluetooth-enabled badges, key-rings or wristbands to record proximity information that can be uploaded to a central database.[43]

Endnotes

1 https://www.gov.uk/government/publications/contact-tracing-letter-to-directors-of-public-health
2 https://www.ft.com/content/4a282a0f-5a9f-4f7d-a313-231975d231bd
3 https://www.bbc.co.uk/news/technology-52381103
4 https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/
5 https://cdei.blog.gov.uk/2020/04/27/how-is-the-cdei-supporting-the-response-to-covid-19/
6 https://www.scer.scot/database/ident-12745
7 https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/
8 https://www.bbc.co.uk/news/technology-52441428
9 https://www.bbc.co.uk/news/technology-52441428
10 https://www.openrightsgroup.org/blog/2020/time-for-a-coronavirus-safeguards-bill
11 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582550
12 https://committees.parliament.uk/event/837/formal-meeting-oral-evidence-session/
13 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (p. 9 and footnote)
14 https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J
15 https://e-estonia.com/trace-covid-19-while-respecting-privacy/
16 https://www.ots.at/presseaussendung/OTS_20200422_OTS0052/stopp-corona-app-weiterentwicklung-mit-hilfe-der-zivilgesellschaft
17 https://www.swissinfo.ch/eng/digital-solution_contact-tracing-app-could-be-launched-in-switzerland-within-weeks/45706296
18 https://www.bbc.co.uk/news/technology-52366129
19 https://github.com/DP-3T/documents/blob/master/Security%20analysis/ROBERT%20-%20Security%20and%20privacy%20analysis.pdf
20 https://risques-tracage.fr/
21 https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
22 https://www.abc.net.au/news/2020-04-26/coronavirus-tracing-app-covidsafe-apple-iphone-covid-19/12187448
23 https://www.legislation.gov.au/Details/F2020L00480/Html/Text
24 https://www.covidsafe.gov.au/help-topics.html
25 https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-agency-response.pdf
26 https://twitter.com/MsLods/status/1254281929513295874
27 https://www.medianet.com.au/releases/186660/
28 https://institute.global/policy/price-worth-paying-tech-privacy-and-fight-against-covid-19
29 https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19
30 https://www.infobae.com/america/agencias/2020/04/26/chile-seguira-con-plan-de-entregar-carnet-de-alta-de-coronavirus-pese-a-advertencia-de-oms-2/
31 https://www.24horas.cl/coronavirus/daza-y-pacientes-asintomaticos-en-chile-no-tenemos-un-numero-fehaciente-de-cuantos-serian-4128843
32 https://onezero.medium.com/immunity-passports-could-create-a-new-category-of-privilege-2f70ce1b905
33 https://osf.io/preprints/lawarxiv/yc6xu/
34 https://www.bbc.co.uk/news/world-52425825
35 https://www.imperial.ac.uk/news/196973/wearable-sensor-trialled-remote-covid-19-monitoring/
36 https://www.comarch.com/press-center/news/corporate/quarantined-sofia-residents-to-receive-comarch-lifewristbands/
37 http://www.isrctn.com/ISRCTN51255782
38 https://www.avawomen.com/press/liechtenstein-study-aims-to-help-combat-coronavirus-pandemic/
39 https://rombit.be/smart-bracelet-to-prevent-coronavirus-infections-in-the-workplace/
40 https://romware.com/covid-radius/
41 https://www.ft.com/content/caeb250b-8d8b-4eaa-969c-62a8b58464aa
42 https://www.locix.com
43 https://www.microshare.io/universal-contact-tracing/
44 https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf
45 https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Exit-through-the-App-Store-Explainer-for-Government-April-2020.pdf
46 https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Exit-through-the-App-Store-Explainer-for-Parliament-April-2020.pdf
47 https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Exit-through-the-App-Store-Explainer-for-Technology-Developers-April-2020.pdf
48 https://www.ipsos.com/ipsos-mori/en-uk/majority-britons-support-government-using-mobile-data-surveillance-tackle-coronavirus-crisis