© University Press 2021
ISSN 2719-6550
ISSN 2719-7417 online

"Journal of Education, Technology and Computer Science"
No. 2(32)/2021
www.eti.rzeszow.pl

Received: 5.10.2021
Accepted for printing: 25.11.2021
Published: 28.12.2021
License: CC BY-SA 4.0

DOI: 10.15584/jetacomps.2021.2.10

CHRISTINE HILCENKO[1,2,3,*], **TARA TAUBMAN-BASSIRIAN**[4], **ZORAN KOVACIC**[5,6]

Covid Tracking Apps, Over Reliance on Technology, Bias and Unfairness

[1] ORCID: 0000-0002-9596-7833, Cambridge Institute for Medical Research, Cambridge, CB2 0XY, UK.
[2] Department of Haematology, University of Cambridge, Cambridge, CB2 0XY, UK
[3] Wellcome Trust-Medical Research Council Stem Cell Institute, University of Cambridge, Cambridge, UK
[4] https://www.datarainbow.eu
[5] School for primary and secondary education with dormitory "Vuk Karadzic", Sombor, Serbia
[6] Secondary medical school "Dr Ruzica Rip", Sombor, Serbia
[*] Presenting and corresponding author

Abstract

Various contact tracing apps tracking the spread of the pandemic were issued in different countries. Mainly based on two technologies, centralised with more control by the governments or decentralised controlled by the Apple or Google Android mobile phone systems. In this paper, we will discuss the advantages and disadvantages of the different systems, as well as their potential dangers.

Keywords: privacy, individual freedom, security, information

I – The choice of the technology and its impact on containing the pandemic

A. Centralised or decentralised APP, protection of collected data

a. All proposed tracing systems process personal data concerning health

The UK ICO (International Association for Cryptologic Research) like the French CNIL (https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet--dapplication-mobile-stopcovid) have expressed their preference for the decentralised model. Chris Pounder sees further vulnerability of the centralised approach with a *"future legislative mood of Government"*. He believes *"It could*

be tempting (e.g. to reduce the pressures on the public purse) for the Government to enact legislation that makes certain processing of personal data compulsory. For instance, to prove entitlement to a COVID related benefit.

Considering to revert to a decentralised model to resolve their Bluetooth issues. "Covidsafe app is not working properly on iPhones, authorities admit" "Australians running the Covidsafe contact tracing app on iPhones may not be recording all the data required if they don't have the app running in the foreground or they are using an older model phone, the government has admitted".

France is struggling to find an agreement with Apple and Google (Kar--Gupta, Rose, 2020) and Australia, who has already deployed the App, has been struggling technically (Tylor, 2020).

The Register (McCarthy, 2020) wrote: *"UK finds itself almost alone with a centralized virus contact-tracing app that probably won't work well, asking for your location may be illegal". "On Monday, the UK government explained in depth and in clearly written language how its iOS and Android smartphone application – undergoing trials in the Isle of Wight – will work, and why it is a better solution to the one by Apple and Google that other nations have decided to adopt. It has also released a more technical explanation".*

Chris Pounder of Amberhawk views that the data subject is identifiable and the data related to medical health. He is therefore *"pretty sure the APP is processing personal data and special category of personal data"*, subject to the Article 6 lawful basis and a condition that overcomes the prohibition in Article 9(1) from processing health personal data, health data benefiting from an extra level of protection under the EU GDPR as a special category data.

Thus, the anonymity of users must be enforced by a combination of legal, technical and organisational measures.

b. The often-stressed voluntariness of the app is illusory

As the emphasis is on the voluntary adoption of the app, the first question is how *data subject consent* is freely given. Chris Pounder points out that *"the NHS test on the website is very careful to avoid the use of the «C word» and it is easy to see why"*.

Many employees will have no other choice than downloading the app. Consent is rarely valid in the employment relationship.

GDPR Recital 43 states with respect to consent that: *"consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller"*. This will be the case where the controller is a public authority or an employer. It will be unlikely for that consent to be considered as *"freely given"*. Therefore, voluntary adoption does not refer to the character of legitimate basis on consent.

The limit of the *"voluntary"* adoption is that it could lead to a denial of a service as previously for the UK *"ID Card holders refused to «volunteer» making it a requirement to interact with any public service"*.

c. The APP should not keep any personal information and no location data. Only the first half of the postcode is collected from APP users to alert local hospitals.

However, for Laurie Clarke reporter, remains:

"Uncertainty over who could access NHSX contact tracing app data as Isle of White pilot goes live". "The NHSX coronavirus contact tracing app is being rolled out on the Isle of Wight this week, but major question marks still hang over the app. Matthew Gould, CEO of NHSX, told parliament today that the data collected by the app would be accessible to unspecified organisations as long as it was used for public health purposes".

B. Efficiency of the tracking app to combat the spread of the virus and the balance of proportionality

Any collection of personal data represents a potential harm to the data subject, especially when data is related to health. The balance of proportionality should therefore be applied.

a. The balance of proportionality requires a three-part test

Fundamental rights, enshrined in the Charter of Fundamental Rights of the European Union constitute the core values of the European Union. These rights must be respected whenever the EU institutions and bodies design and implement new policies or adopt any new legislative measure and in the European Charter of Human Rights.

European Union law which requires that *"the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties"*.

"The principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives". It therefore *„restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or Under Article 52(1) of the Charter, "subject to the principle of proportionality, limitations on result reached)" the exercise of fundamental rights may be made only if they are necessary (...)"*.

1. The necessity, something needed to be done to end this national confinement killing the country's economy.

See the Data Protection Impact Assessment published by the Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. (Bock et al., 2020). They recommend that:

- An appropriate legal basis must be established and, in this respect, responsibilities have to be defined.
- Reinforcing the measures of pseudonymisation "when creating the TempIDs in the app, it must be ensured that there is no connection between TempIDs and it must never be possible to make one. … The server(s)' operator must employ an effective separation method..."
- Accompanying the publication of the app it must be ensured in law and in fact that users have to disclose neither the status of the app nor the mere existence of a device to third parties.
- Before the app gets published, a comprehensive investigation of the software and the overall system must be conducted and published by an independent body.

The first comment is that any interference by a public authority is unlikely to infringe Article 8(1) of the European Convention on Human Rights; This is because Article 8(2) permits legislation to be enacted by a Parliament process (*e.g.* in the Coronavirus 2 which sets aside the A.8(1) right in limited circumstances (e.g. any interference deemed necessary *"for the protection of health"*). The requirement is based on the criteria of necessity. If there is reliance on data subject consent (which we have demonstrated above that is unreliable), then there is also no Article 8 breach (so long consent is properly formed).

Based on the GDPR, *"if the processing is «necessary» it will have Article 6 lawful basis (e.g. candidates are Article 6(1)(c) or Article 6(1)(e); Article 6(1)(d) could be used in a case-by-case emergency). If there is a need for an Article 9 condition that lifts the prohibition on processing of health personal data the candidates are Article 9(2)(c), Article 9(2)(g), Article 9(1)(i)".*

"If there is reliance on consent or necessary or public task (or even necessary legitimate interests of controller/Third Party), the controller has to specify publicly (A.13; A.14) what happens to the personal data if there is withdrawal of consent or exercise of the exercise of the right to object to the processing".

Therefore, he concludes *"the ICO should take up Article 8 ECHR cases on the grounds that necessary as used in the GDPR has the same meaning as in Article 8".*

2. Could the same result be achieved in a less intrusive manner?

We would argue providing tests, masks, ventilators and resources to overloaded European health systems could bring a serious improvement without any inconvenience.

The cost of the deployment of the tracing APP is unknown. The Australian Government would have allegedly spent 700.000 AUD just to host the data on Amazon AWS clouds. These funds will escape the health system.

A letter, signed by 177 scientists and researchers working in the UK in the fields of information security and privacy, reads:

"Echoing the letter signed by 300 international leading researchers, we note that it is vital that, when we come out of the current crisis, we have not created a tool that enables data collection on the population, or on targeted sections of society, for surveillance. Thus, solutions which allow reconstructing invasive information about individuals must be fully justified.1 Such invasive information can include the «social graph» of who someone has physically met over a period of time. With access to the social graph, a bad actor (state, private sector, or hacker) could spy on citizens' real-world activities".

Actually, early testing can give far better results as epidemiologists are saying it is during the first 24 hours that the COVID+ are most contagious. *"Coronavirus: Send virus alerts within 24 hours or risk a second wave, scientist warns"* (Fraser, 2020).

b. Without a capacity to intervene and a narrow purpose limitation, the protection of fundamental rights will be at stake.

Wired magazine wrote: Coronavirus contact tracing apps were meant to save us. They won't (Burgess, 2020). *"With little evidence to show how effective such apps are and growing privacy concerns, there's a risk they could do more harm than good".*

From Iceland to Israel, more than 30 systems are being developed by governments and health authorities. They promise to automate the laborious process of tracking down the contacts of infected individuals, helping to slow the spread of coronavirus through the population and save lives.

False alerts might lose users' trust. According to an Oxford research, the probability of seeing any result from the tracing Apps requires that at least 60% of the population use the App. Will the most vulnerable population of over 60s be willing to download and know how to use the APP? Will the government be liable for the false alerts causing distress, unnecessary isolation and loss of revenues? France is talking of self-isolating in hotels, where and how to feed and entertain these people?

<u>Projects using personal data to combat SARS-CoV-2</u>

Singapour's TraceTogether App (https://support.tracetogether.gov.sg/hc/en--sg/articles/360046475654-20-April-2020-One-Month-On) *moved to the The Apple and Google collaboration on digital contact tracing solutions, is a game--changer, as we said previously. It will significantly improve the contact tracing*

capability available to governments and public health authorities over what is available through public APIs on either Android or iOS platforms. We are glad that Apple and Google are engaging governments and public health authorities around the world, including us, to incorporate feedback as the specifications for their contract tracing protocol and private APIs.

In Poland (https://www.lexology.com/library/detail.aspx?g=e6e61ca3-45ae--49a0-b6f1-5fd4adf11291), although initially voluntary in nature, it has become mandatory for all those under obligatory quarantine or epidemiological surveillance, as a tool to confirm compliance with quarantine obligations (*e.g.* whether the ban on leaving the quarantine location is observed).

Contact tracing apps in Austria: a Red Cross initiative has been launched In March 2020 in co-operation with Accenture.

The first published version of the Stopp Corona app required users to log their contacts via a "manual" handshake. In the current version, however, the app already allows contacts to be traced automatically, depending on the device and its configuration.

The automatic handshake functionality is based on the discovery and messaging functionality of the p2pkit developed by the Swiss company Uepaa, which uses Bluetooth and Wifi-direct techniques to determine the distance between the users.

Switzerland: "WeTrace" app (Private)

This project is ready to be deployed. It is open source. All data remains locally on the devices. Packaged information encrypted asymmetrically. The sole information a potential malfeasor on the central server would see is the fact _that_ an infected person has actually pushed a status update, but on the core server it is not visible "what" the person has broadcasted. The broadcasting user can determine the details of what should be broadcasted aside from status (location of contact, time of contact, etc.). Packages will be sent not to everyone but only to those that need to know.

Spain: "Open Coronavirus" app (Private)

The Spanish medical investigator Aurelia Bustos has released Open Coronavirus, an open-source app with the aim to copy the advantages of the South--Korean app: in the end, serving as an individual-validation-method in order to allow free movement of the citizens. This tool can be used by any public institution as a basis for its own apps on tracking citizens due to the coronavirus emergency, and it offers a modular design: three levels of management (mobile phone, central management of data by the competent authority and checking of the control points by the competent authority too) with different options of geolocation (GPS, bluetooth, positioning by mobile operators cells) that could be

implemented or not by the corresponding institution. Its use would be voluntary for the citizen (although, in words of the medical investigator, "it would be probably very advantageous for the user, as it would allow him/her to have the possibility to finish an eventually longer quarantine"), and it would necessarily depend on the realization of any kind of coronavirus detection tests.

As this is an open-source app, it will not be officially published in its current status, and any use of the same by any institutions must be always in line with GDPR.

Sadly, it can be said of the NHSX Tracing App, similar to the French STOPCOVID. « StopCovid est un projet désastreux piloté par des apprentis sorciers » (https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-est-un--projet-desastreux-pilote-par-des-apprentis-sorciers_6037721_3232.html).

II – The question of over-reliance on technology

A. The margin of error imposing unfair self-isolation

a. The APP has encountered technical issues

Running the Bluetooth connection in the back has several inconveniences such as draining the battery and opening security vulnerabilities.

b. The margin of error is inherent to the technology

The Bluetooth distance measurement is unreliable according to its own inventor (https://www.nu.nl/tech/6046965/bluetoothuitvinder-gebruik-bluetooth--voor-corona-app-niet-erg-nauwkeurig.html). Bluetooth signals can pierce obstacles such as a wall, glass or vehicle bodies, the virus expectedly cannot such as a wall or vehicle bodies.

The margin of error has caused a return to lock down in Singapore, one of the first nations after China to deploy the TraceTogether App. Less than 20% of the population actually downloaded the App It is suspected that Bluetooth works through glass and even some walls and may even be triggered by reflection in windows in buildings. Jason Bay Senior Director (Government Digital Services) at the Government Technology Agency, Singapore wrote (https://blog.gds--gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98):

*If you ask me whether any Bluetooth contact tracing system deployed or under development, anywhere in the world, is ready to replace manual contact tracing, I will say without qualification that the answer is, No. Not now and, even with the benefit of AI/ML and – God forbi – blockchain? (throw whatever buzzword you want), not for the foreseeabl*e future.

The number of **false alerts** will cause major distress and reduce trust on the App. When someone receives the warning SMS that they have been in contact with someone COVID+, that doesn't mean they can be immediately tested. They

might be asked to self-isolate something not always practical. It has been suggested in France to allocate hotel rooms to quarantine. That means 14 days of accommodation, food and entertainment. During that time the individual and his family or network will be under distress, maybe unnecessarily isolated causing loss of revenues. Should the government be liable for these consequences?

B. Unfairness caused by discrimination against

The often-stressed voluntariness of the app is illusory

a. In the employment context, voluntariness is an illusion.

The APP with its errors can lead to unfair situations for employers discriminating if they refuse the APP or when mistakenly out spotted.

b. The extension of the contact tracing apps with the COVID vaccine passport expands the discrimination especially as not the entire population has benefited from the vaccine.

Restraining access to services or public places based on the vaccine is discriminatory therefore unfair.

c. **These Apps are source of security issues difficult to handle for non--techy users**

The main public targets are the less tech savvy. Not everyone owns a smartphone and even many over 50's would not be able to technically set their smartphone securely.

Lizzie Dearden (https://www.independent.co.uk/author/lizzie-dearden), Security correspondent for the Independent reports : *"malicious false alerts"*, warn experts. *"Individuals could send out false alerts causing people to self-isolate unnecessarily and hackers could generate «proximity events» ... because users can set off the warnings themselves by reporting symptoms – rather than positive Covid-19 test results – it could be used to send out false alerts"*. Or *"People can deliberately put others into quarantine or report large areas", he said. "A child could try to get a day off school by reporting symptoms from a parent's phone to trigger a quarantine"*.

"Dr Michael Veale, a lecturer in digital rights and regulation at University College London who this week gave evidence to MPs on the technology, told The Independent that Britain's tracing app had nothing to stop individuals «maliciously triggering notifications» using its normal functionality".

The well-known security and privacy expert and fellow at the Berkman Klein Centre for Internet & Society at Harvard University Bruce Schneier has expressed his concerns about the issues of using Bluetooth Technology (https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html).

"My problem with contact tracing apps is that they have absolutely no value". He told BuzzFeed News: *"I'm not even talking about the privacy concerns; I mean the efficacy. Does anybody think this will do something useful? ... This is*

just something governments want to do for the hell of it. To me, it's just techies doing techie things because they don't know what else to do".

SecurityWeek reporter Kevin Townsend wrote (https://www.securityweek.com/covid-19-contact-tracing-apps-effective-virus-risk-management-tools-or-privacy-nightmare): *"These apps could easily become subject to a high number of false positives – and false positives always lead to a rejection by users".*

Sean Lyngaas wrote in Cyberscoop (https://www.cyberscoop.com/bluetooth--exploit-jan-ruge-contact-tracing/): As contact tracing gains attention, a researcher pokes a hole in Bluetooth technology. The article cites *"Jan Ruge, a researcher at the TU Darmstadt, a university in Germany, has shown how a hacker in close proximity to an Android device could use Bluetooth to execute code on it. The mobile device's user wouldn't need to click on anything to be compromised – the attacker would only need the Bluetooth address of the device and a software exploit. Ruge used the exploit on a Samsung Galaxy S10e, but it would work in theory on other phone models running unpatched versions of the Android 8.0–9.0 operating systems".*

Any database inherently creates security issues.

Constant Bluetooth signals in the back will drain the phone battery eventually causing overheating. Will we witness a new pandemic of "pockets in fire"?

d. Constant monitoring of the general population has impacts on individual freedom

ICAR, the Association of experts in Cryptologic research has issued a statement against mass surveillance " (https://www.iacr.org/ misc/statement-May2014.html):

- *The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards. Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.*

A technical deep-dive into the NHS COVID-19 contact tracing app (https://reincubate.com/blog/nhs-covid-19-background-tracing-details): Since *"the contact tracing beta is now open source for both iOS and Android, along with some documentation. As a follow-up to our «Staying alive» post* (https://reincubate.com/blog/staying-alive-covid-19-background-tracing/)*, we've taken a deep--dive into the source code. It's pleasantly surprising to find it licensed under MIT, indicating an NHSX commitment to transparency and quality... There have been claims that the Android app accesses location data, as the prompt for Bluetooth API access on Android devices appears to ask for location permissions. However, we debunked this yesterday: this is a consequence of how Android manages requests for Bluetooth permissions".*

Reincubate's CEO, Aidan Fitzpatrick, says:

Yes, it is the case that the coming Apple Exposure Notification framework in iOS 13.5 obviates the need for these keepalives. However, it's worth noting that:

- iOS 13.5 has not been released, and may not be for some weeks
- Prior to yesterday, the last iOS 13.5 beta had a major security flaw, suggesting heavy lifting is going on in Apple's engineering teams
- Once it is released, it will likely take months for a majority of iOS users to install it (unusually, the equivalent Android adoption may be more rapid)
- Older iOS devices – such as the iPhone 6 – cannot run iOS 13, and will not be able to use the Apple technique
- *There's no reason why the NHS COVID-19 app won't be able to automatically transition in future to using Apple's framework – or even dual-running both mechanisms.*

The app will become increasingly effective as more people use it, and the benefit of mass adoption will create a flywheel effect in this sense. The Australian COVIDSafe app struggled as it didn't support detecting backgrounded iOS devices from an Android device, and it didn't have this clever iOS-to-iOS keepalive mechanism.

C. Masks and COVID tests versus tracking

After a year of pandemic, tracing APPs did not show much efficiency. Masks, tests and vaccines were needed with higher results. The all-technology solution as the French CNIL had warned was a costly dream.

D. The more human friendly option of dog sniffing COVID

Testing and isolating infected populations could have been achieved in a little intrusive and economically affordable manner by trained. Nicholas, The Guardian correspondent wrote "Any breed could do it": dogs might be a Covid tester's best friend. *"It is simple and pain-free, could be used to test for coronavirus in care homes, airports and schools, and might just be more realistic than the UK government's £100bn «Operation Moonshoot» mass screening plan. Its name? Fido".*

Conclusion

It's important to reflect on which circumstances make use of technology like this appropriate. If contact tracing is successful in saving lives, which criteria should be assessed as to whether it's applied for future diseases? Once the precedent is set, is there an argument that this technology might be used to combat *pre-existing* infectious diseases? It's foreseeable that different societies will evaluate the trade-offs differently.

References

Bock, K., Kühne, C. R., Mühlhoff, R., Ost, M. R., Pohle, J., Rehak, R., (2020). *Data Protection Impact Assessment for the Corona App*. Retrieved from: https://www.fiff.de/dsfa-corona (8.07.2021).

Burgess, M. (2020). Coronavirus contact tracing apps were meant to save us. They won't. https://www.wired.co.uk/article/contact-tracing-apps-coronavirus (10.05.2021).

Fraser, Ch. (2020). Coronavirus: Send virus alerts within 24 hours or risk a second wave, scientist warns. https://news.sky.com/story/coronavirus-send-virus-alerts-within-24-hours-or-risk-second-wave-scientist-warns-11984908 (14.09.2021).

https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98 (2020) (8.09.2021).

https://reincubate.com/blog/nhs-covid-19-background-tracing-details (2020) (6.08.2021).

https://reincubate.com/blog/staying-alive-covid-19-background-tracing/.

https://support.tracetogether.gov.sg/hc/en-sg/articles/360046475654-20-April-2020-One-Month-On (2020) (6.08.2021).

https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid (14.09.2021)

https://www.cyberscoop.com/bluetooth-exploit-jan-ruge-contact-tracing/ (2020) (12.08.2021).

https://www.iacr.org/misc/statement-May2014.html (7.07.2021).

https://www.independent.co.uk/author/lizzie-dearden.

https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des--apprentis-sorciers_6037721_3232.html (2020) (15.06.2021).

https://www.lexology.com/library/detail.aspx?g=e6e61ca3-45ae-49a0-b6f1-5fd4adf11291 (18.08.2021).

https://www.nu.nl/tech/6046965/bluetoothuitvinder-gebruik-bluetooth-voor-corona-app-niet-erg--nauwkeurig.html (2021) (15.07.2021).

https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html (2020) (14.08.2021).

https://www.securityweek.com/covid-19-contact-tracing-apps-effective-virus-risk-management-tools--or-privacy-nightmare (2020) (16.07.2021).

Kar-Gupta, Rose (2020). France accuses Apple of refusing help with "StopCovid" app. *Technology News.* https://www.reuters.com/article/us-health-coronavirus-france-tech-idUSKBN22H0LX (21.09.2021).

McCarthy, K. (2020). UK finds itself almost alone with a centralized virus contact-tracing app that probably won't work well, asks for your location, may be illegal. *The Register*. https://www.theregister.com/2020/05/05/uk_coronavirus_app/ (1.09.2021).

Taylor, J. (2020). Covidsafe app is not working properly on iPhones, authorities admit. *The Guardian*. https://www.theguardian.com/world/2020/may/06/covidsafe-app-is-not-working-properly-on-iphones-authorities-admit (8.09.2021).