Use of participatory apps in contact tracing

Options and implications for public health, privacy and trust

Buchanan, W., Imran, M., Pagliari, C., Pell J. & Rimpiläinen, S.

2nd June, 2020

Authors

Buchanan, William[1], Imran, Muhammad[2], Pagliari, Claudia[3], Pell Jill[4] & Rimpiläinen, Sanna[5].

1 School of Computing, Edinburgh Napier University; 2 James Watt School of Engineering, University of Glasgow; 3 Usher Institute, University of Edinburgh; 4 Institute of Health and Wellbeing, University of Glasgow; 5 Digital Health & Care Institute, University of Strathclyde.

For referencing, please use:

Buchanan, W., Imran, M., Pagliari, C., Pell J. & Rimpiläinen, S (2020). *Use of participatory apps in contact tracing – options and implications for public health, privacy and trust.* Digital Health and Care Institute, University of Strathclyde, Glasgow. https://doi.org/10.17868/73197

Disclaimer

Copyright

First released June 2nd, 2020.

First published July, 14th, 2020.

Table of Contents

Introduction

On December 31st, 2019, the World Health Organisation received a report from the Chinese government detailing a cluster of cases of 'pneumonia of unknown origin', later identified as novel coronavirus. The virus, now referred to as COVID-19, quickly spread and was officially declared a global pandemic on March 11th.

COVID-19 has put health services under enormous strain globally. Turning to digital methods for collating data on cases, associated symptoms and the routes through which the virus may be spreading has been a common response.

Human-powered contact tracing, although resource-intensive, is still considered to be the most effective way of tracking and helping to curtail the spread of infectious diseases[i]. Intense efforts are underway to develop digital tools that can augment and automate some of these processes, such as the NHSX app or Singapore's TraceTogether app, however, these are often beset with technical and privacy-related issues.

This report reviews digital approaches that involve citizens as co-actors in efforts to support contact tracing, which may include elements of both location/proximity monitoring and symptom reporting, the latter representing a type of crowdsourced disease surveillance.[ii] This is approached from the perspectives of public health data needs, privacy-centred architectures, technologies and standards, and digital ethics.

The aim is to inform an approach to digital contact tracing that is consistent with Scottish policy around secure, transparent, participatory and privacy-respectful data sharing for health and wellbeing. As such, some of the insights and recommendations are applicable to broader aspects of digital health in Scotland.

The report collates expert answers to the following questions:

- What are the desirable outcomes arising from the automation of symptom and contact tracing data collection at scale? (Prof Jill Pell, Institute of Health and Wellbeing, University of Glasgow);
- How might the distributed system be architected to be secure and respectful of privacy from the outset? (Prof Bill Buchanan, OBE, School of Computing, Edinburgh Napier University);
- What communications standards and methods would best support the approach? (Prof Muhammad Imran, James Watt School of Engineering, University of Glasgow);
- What are the ethical challenges and what steps should Scottish Government take to secure public trust? (Prof Claudia Pagliari, Usher Institute, University of Edinburgh)

What are the desirable outcomes arising from the automation of symptom and contact tracing data collection at scale?

(*Jill Pell, Institute of Health and Wellbeing, University of Glasgow*)

From a health system perspective, desirable outcomes of digital COVID-19 apps fall into three main categories: Public Health (enabling case finding and contact tracing), Clinical and Self-management (informing risk predictions and interventions), and Service Planning (estimating prevalence and patterns to aid planning and policy).

Public Health

Case finding, contract tracing and isolation are now widely agreed to be central to reducing the transmission of infectious diseases. Countries that had sufficient testing capacity to implement this strategy at the outset of COVID-19, such as South Korea[iii], have experienced fewer cases and fewer deaths. UK and Scottish testing capacity have increased greatly since the onset of the pandemic, with thousands of additional tracers having recently been recruited, which will be vital to support any lifting current restrictions (i.e. exiting lock-down).

Currently, many symptomatic people are self-managing without presenting to the NHS and many people who may have been infected will not be aware of this. An app that can be used by members of the public may prove valuable for identifying possible/probable community-based cases currently unknown to the NHS. It could also be used to provide these people with immediate advice on social distancing prior to receiving a test result, provide more rapid communication of positive test results, help with identifying the contacts of confirmed cases, and facilitate their testing and advice.

The potential benefits therefore include reduced community transmission and prevention of a resurgence of cases and deaths when current restrictions are lifted.

Clinical and self-management

Identification of the risk factors associated with having a poor outcome following COVID-19 infection has been highlighted as a priority for COVID-19 research[iv], because it can support better decisions about when and how to intervene. A recent systematic review found no risk prediction models for COVID-19 assessment outside of hospitals.[v] Hospitalised patients are a highly selected sub-group of patients and risk models developed in these patients may not be generalisable to patients in the community. Information collected using an app could help to develop these community-based risk models.

A suitable app would give people who have tested positive a means to report others they have recently been nearby, so the NHS can contact those people by telephone with advice to self-isolate. Contacts can also use such an app to monitor their own symptoms and seek support if these escalate. Some apps also seek consent from users to link the symptom information they provide to their other health records, including not only test results but also information on hospitalisation, admission to ICU, ventilation, length of hospital stay and death. The data obtained could then be used in research to develop community-based risk models, which could be built into the app to provide patients who are self-managing with more appropriate recommendations on when to seek advice, assessment and testing. The same information could be used by community-based healthcare staff to inform their triage decisions.

The benefits therefore include the development of evidence-based risk prediction tools that improve self-management and clinical decision making; improving patient outcomes whilst reducing the risk of overburdening health services through avoidable referrals.

Service planning

There is currently a lack of UK data on the true incidence of COVID-19. Many cases currently do not present to the NHS and are not tested. Attempts have been made to infer population incidence from prevalence data, or incidence among the sub-group of patients who are tested, or from our understanding of other viral respiratory infections. Wide-scale use of an app that records the start date of symptoms, rapid testing of index cases and collection of symptoms among contacts would provide much better information on, and tracking of, population incidence. This in turn would inform our understanding of:

- When and where to enhance or lift restrictions;
- The testing capacity required to implement case finding and contact tracing;
- Testing strategies; and
- The location of testing facilities.

Given the current situation of incomplete case ascertainment and highly selected data collection, the classification of a "very high risk" sub-group of the population in need of shielding has been based on expert opinion informed by previous viruses and limited information on COVID-19 collected in other countries.

Collection of standardised data on a more complete and representative sample of cases would enable us to produce more evidence-based definitions of those groups in needs of enhance shielding when current restrictions are lifted.

How might the distributed system be architected to be secure and respectful of privacy from the outset?

(*Bill Buchanan, School of Computing, Edinburgh Napier University*)

There are two main options available for automating contact-tracing: one where identities are unknown (e.g. strangers co-located on public transport) or one which present unacceptable privacy barriers (e.g. precise location monitoring is unacceptable in the UK). Both are based on the exchange of anonymous, temporary 'Bluetooth handshakes' between mobile phones. The 'decentralised' model favoured by **Google/Apple** keeps all data on the phone, which apps can only access via a secure API with the user's agreement. In contrast, the **NHSX** App requires direct Bluetooth access and holds a copy of users' cryptographic 'identity' on an NHS database, so that this can be linked with other services or information for supporting human contact tracing, analytics or research.

The NHSX App allows the health service to perform matches and follow-up on contacts but suffers from many technical problems related to it being a stand-alone application. The installation of the App from an App store will be a significant barrier, along with the complexity of setting up the rights to monitor contacts. The Google/Apple API has strong privacy settings, but will not allow the NHS to follow-up on contacts, unless consent is built in.

Some significant points are:

1. **Decentralised tracing:** The Google/Apple contact tracing method has strong privacy protections built in: the data collected is stored locally on the app user's device, and

user's consent is required for the release of infection data. On infection, a diagnosis key is sent to the NHS and this is held within a public repository. Everyone with the App can then determine if they are, and were, in contact with someone who is infected, but only for one day at a time. While secure for the user of the app, this approach has the disadvantage over the centralised approach, such as used by the NHSX app, in that the public health authority will not be able to use this data for contact tracing.

2. **Centralised tracing:** With the **NHSX App**, users register and are assigned a unique ID on a central server (**InstallationID)**. The NHS can then track the identity of people involved in a contact while using the app. Overall consent is added through the installation of the App. There are a number of security concerns around the NHSX App:
    a. Storage of the identifiers and the length of time that data gathered around the identifiers will be used on a centralised server.
    b. Concerns over the potential leak of the private key of the NHS, and which could possibly reveal all of the contacts. This is because public key encryption is used in the NHSX App, and where the public key is sent to the App, and which is then used to protect the identity as it is passed back to the central server. A breach of the associated private key would allow anyone to decrypt the identity passed back.
    c. Concerns that the data will not be sent directly to the NHS, but would be gathered by a third-party organisation, and stored within the public cloud.
3. **Local tracking**: The Google/Apple API uses a rolling identifier that allows a user to be traced locally for only 10 minutes at a time, whereas the NHSX App uses a daily public key which can be resolved back to the user. There are thus concerns that a citizen could be tracked locally for one day with the NHSX App, as their associated daily public key is exposed for that time.
4. **Bluetooth stack:** With the **NHSX App**, a significant worry is that it has its own Bluetooth stack, and which is not embedded into the operating system of the phone. This could pose security risks for fake apps and in the power drain of the device. If the drain is too large, users may end-up turning off their Bluetooth, or even uninstalling the App. As the UK needs at least 60% of the population to install the App for it to be an effective means of contact tracing, this may have a significant impact on the trust levels on the NHSX App.
5. **Consent for tracing:** With the Google/Apple API, the contact tracing integration is embedded into the operating system of the phone, and thus has high trust levels, and where a user simply flips a consent switch (Figure 1). For the NHSX App, the App itself must gain the required rights to have full access to the Bluetooth stack, which may require a more complex setup for giving consent.
6. **Length of time for the contact logs to be stored:**
    a) The Google/Apple API stores the contact logs for two weeks and then deletes these for each of the contacts.
    b) As the NHSX App is a stand-alone application storing the data centrally, it can set its own time limits on the time it keeps the contact logs, and the logs which are uploaded to the HA (Health Authority). Contact tracing logs may be kept up to 28 days on the NHS servers. There are questions around the auditing of this information.
7. **Data stored in the public cloud for NHSX App.** It is reported that the data gathered from the NHSX App is being stored in a public cloud run by a private company (Box 1).

Recommendation: The best solution may be to use the Google/Apple API, with consent in the sharing process, but NHSX is the best for workflow (being able to map the steps and

consents). In Scotland, if the NHSX App is to be used, the data should be stored by **NHS Scotland data infrastructure**, and not by an external partner.

> In the NHS app, the infrastructure on which the various back end services operate is run in commercial public cloud, with the NHS in control of the code, deployment, operation and administration of the various infrastructure and services (either directly or through contracts).

Box 1: Text from NHSX Technical Specification

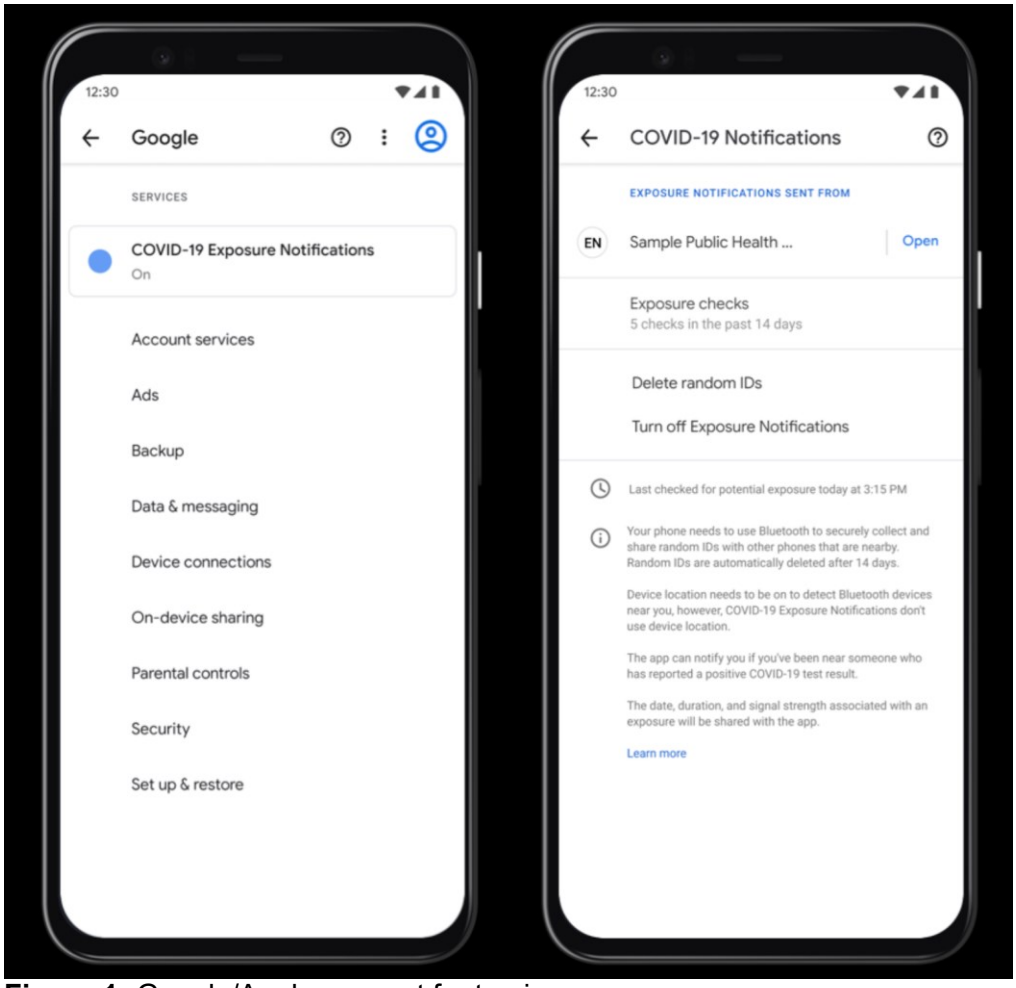


Figure 1: Google/Apple consent for tracing

What communications standards and methods would best support the approach? What initiatives or options are already progressing that may help us get further faster?

(Muhammad Imran, James Watt School of Engineering, University of Glasgow)

Even with the government hiring thousands of new contact tracers, manual methods may be insufficient if infections surge. This is when apps may help to bridge the gap. Table 1 is a list of named apps that are being used in different countries, some of which are explicitly designed to aid contact tracing and others which support other forms of data collection for public health surveillance.

TABLE 1 COVID-19 APPS IN DIFFERENT COUNTRIES

Country	Name of App	Enabling Technology or Method
Global	Apple/Google API	Bluetooth
The UK	C-19 COVID Symptom Tracker	Self-reporting questionnaire
	NHSX	Bluetooth
	Babylon COVID-19 Care Assistant	AI, live chat with human agent, ChatBOT
The EU	Pan-European Privacy Preserving Proximity Tracing Initiative	Open source Bluetooth based sharing platform
8 countries	DP-3T	Bluetooth
France	Covidom	Digital online questionnaire
Poland	Home Quarantine	Instagram's geolocation and facial recognition
Germany	Corona Data Donation	Wearables
Russia	Russian Social Monitoring	Hybrid (GPS, network, Bluetooth, camera)
China	Health Code	GPS, Financial transactions, Mobile network
South Korea	Corona 100m	GPS
	Safety Protection	GPS
Singapore	TraceTogether	Bluetooth

India	AarogyaSetu	GPS, Bluetooth
	COVID-19 Quarantine Monitor Tamil Nadu	GPS
The USA	Safe Paths	Bluetooth
	How We Feel	Online questionnaire
	Private Automatic Contact Tracing	Bluetooth
Iran	contact tracing App	GPS
Israel	Hamagen	GPS
Australia	COVIDSafe	Bluetooth

Understanding patterns of proximity is central to any contact tracing approach, including those involving apps**.** A number of different methods are available to make this possible.

Universal usage of mobile devices, smartphones and internet, GPS, Bluetooth beacons, WiFi, RFID, Telcom Cell Towers, wearable devices, crowdsourcing of social media and tracking of financial transactions can all potentially be used to track a COVID-19 patient's location and that of other people they may have come into contact with.[vi]

GPS, WiFi routers and cell towers provide *absolute location data* in the form of geolocation coordinates while Bluetooth pairing gives *relative location data* in the form of some *reference description* of the location, for example, that both persons shared the same bus.

The **GPS receiver** can compute its position in terms of latitude, longitude, height and timing offset between the receiver and the satellites based on the signals from four GPS satellites. On contrary, contact tracing leveraging **Bluetooth** passively collects information about surrounding Bluetooth IDs by doing regular scans. The phone then stores the list of Bluetooth devices it has encountered (Figure 1).

(a) (b)

Figure 1: Contact tracing using GPS and Bluetooth.

Ubiquity of **WiFi** access through massive deployment of WiFi routers can be exploited to gain the knowledge of a user's mobility data. Using Received Signal Strength Indication, MAC address, personal information and timestamps for the probe request of a user, the router can easily generate a WiFi signal map detecting the location of the user and duration of his presence based on the services used (Figure 2).

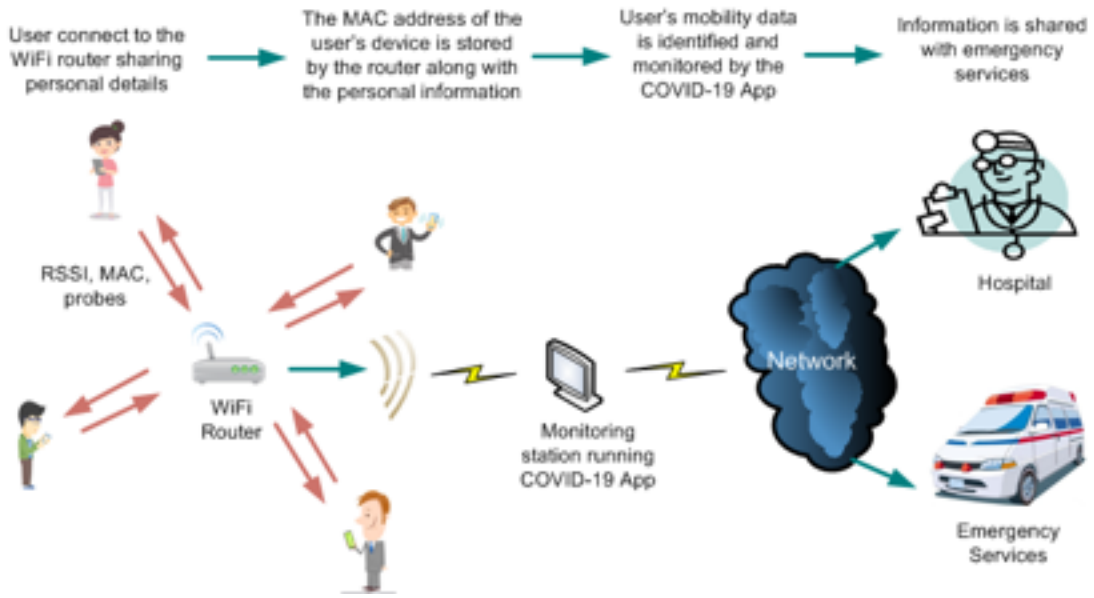


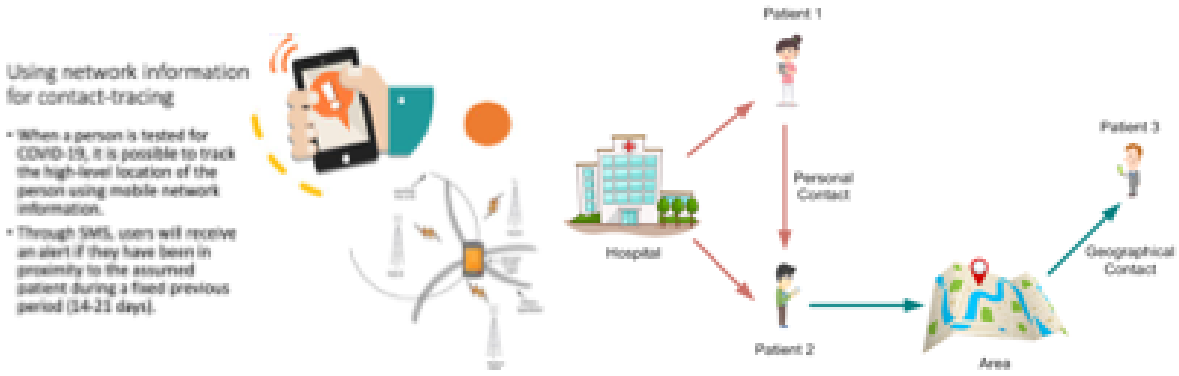
Figure 2: Contact tracing using Wifi.

The **Radio Frequency Identification (RFID)** reader generates a query signal towards the RFID tags and the tag replies back with data. UHF RFID uses passive tags attached to smartphones and objects. It enables location tracking of the COVID-19 patient, as well as items touched/used by them (Figure 3).

Figure 3: Contact tracing through RFID.

5G networks use large antenna arrays and ultra-wide bandwidths (UWB). They enable a decimeter level accuracy in location systems. Mobile network information and radio control signals can also be used to get a subscriber's location and mobility history, as shown in Figure 4 a.

Social media analytics can be expanded by fusing together additional data sources, such as License Plate Recognition, smart city CCTV, ATM transactions and credit card purchases. Graph theory leveraging "small-world network" approach along with mobile network data/WiFi can enable to detect geolocation and contact people information of an individual (Figure 4b).



(a) (b)

Figure 4: Contact tracing using mobile network and social media.

Wearable devices make use of a number of technologies including cellular, Near Field Communication (NFC), Bluetooth, WiFi, GPS, Ultra-wideband (UWB), Long Term Evolution (LTE) and 5G for information gathering, communication and localisation. A typical wearable device can perform the contact tracing feature for COVID-19 by tracking the location of the user through GPS tracker as well as proximity sensors utilising Bluetooth, UWB radio and LTE/5G connectivity (Figure 5).

Artificial Intelligence based technologies such as **facial recognition** can also be employed to identify individuals or reduce the number of false positives, although limited availability restricts their usage.

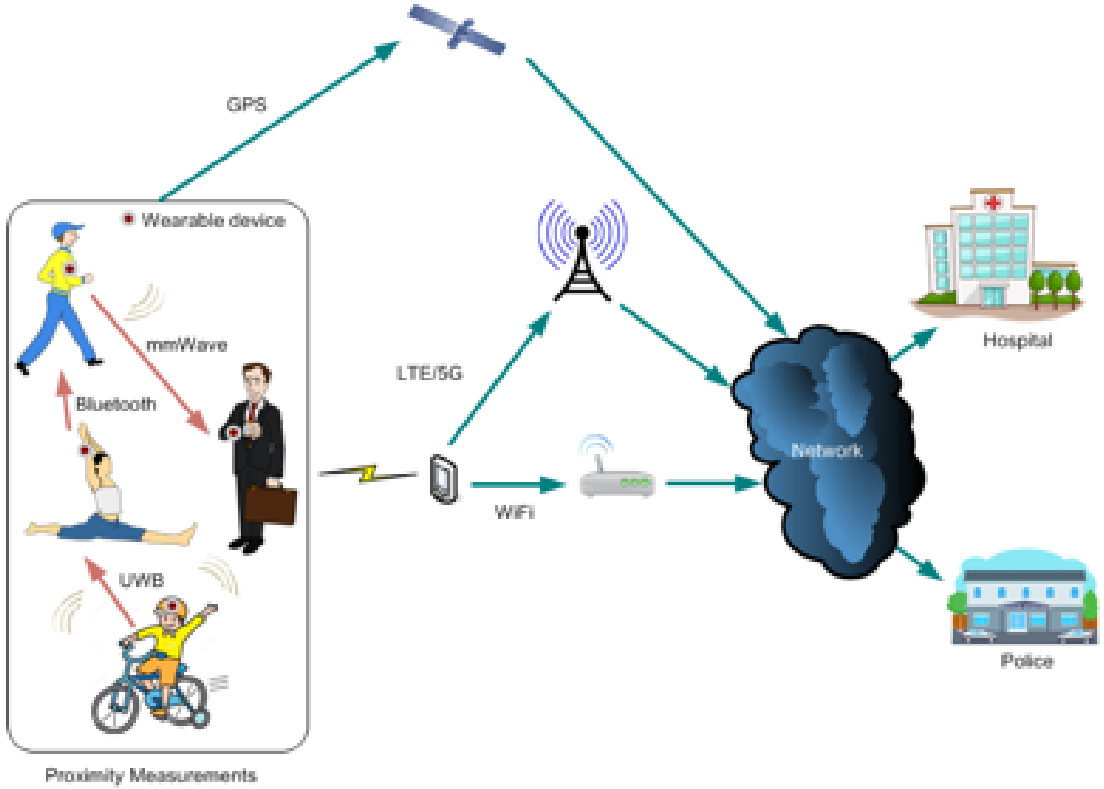


Figure 5: Contact tracing via wearables.

Table 2 summarises the discussed contact tracing enablers along with their advantages and disadvantages. The Bluetooth approach, being pursued at various stages by governments across Europe and Latin America, as well as in Australia and Asia, has emerged as the most

suitable method for contact tracing in the backdrop of COVID-19. However, it has its own deficiencies that limit its capabilities. It requires a majority of people in a geographic area to adopt it for it to be effective. These apps are also considered to be interfering with vital signs monitoring applications, such as diabetes monitoring. Some countries, including South Korea and Israel, are using high-tech methods of contact tracing that involve tracking peoples' location via phone networks. However, such centralized, surveillance-based approaches are viewed as invasive and unacceptable in many countries for privacy reasons. The Bluetooth-based apps are also more privacy-friendly than tracking techniques that use GPS or mobile phone data. They use Bluetooth to broadcast and receive an encrypted, pseudonymous signal from nearby phones and create a log of interactions that remain on the phone, so users' names and numbers are not disclosed.

WiFi is widely available and can be used without any investment in the infrastructure. However, it suffers from low accuracy as its range is 80-100m. Hybrid techniques such as using the built-in accelerometer and gyroscope with WiFi can improve accuracy. Social Media approach also has good potential but is marred by authentication restrictions. Wearables appear to be a dynamic and effective solution as they have the capability to make use of multiple technologies with improved efficiency and higher accuracy.

Contact tracing solutions do not have a uniform system architecture. Whilst countries rush to deploy contact tracing apps, they raise a multitude of issues including privacy, data protection, security loopholes, lack of testing and part use of the smartphones. The privacy concerns need to be eradicated through GDPR compliance, transparent development of the app and data usage and reassurance about the temporary nature of the surveillance. In the light of this discussion, we can make the following recommendations:

- Use of RFID and other technologies for tracing in safe workplaces.
- Use of smartphone's built-in sensors (for example gyroscope and magnetometer) to correlate similar locations without revealing the actual coordinates.
- Optimised use of general Bluetooth technology with a control on range for improving the detection accuracy or combining this with other presented enabling technologies to improve the accuracy and maintain the enhanced privacy.
- Multilayer hierarchy to provide options to end-users to control the comfort level of what is acceptable for them to consent to (lowest layer RFID in workplace only, Bluetooth on users control, Bluetooth pushed by the App with no control, Bluetooth + GPS + RFID).

TABLE 2 COMPARISON OF COVID-19 CONTACT ENABLING TECHNOLOGIES

Technology	**Pros**	**Cons**
GPS	• Locating infected users in real-time. • Identify virus hotspots with Geo-data. • Local information and awareness for patients, carers. • Enables geo-fencing through user monitoring.	• High power, storage and computational requirements. • Low accuracy in urban and indoor. • Social fears of being tracked and lack of trust in the use of personal/health data.

Bluetooth	• Wide availability. • Low power, storage and computational requirements. • List of all devices that have "made contact" is readily available.	• Inaccuracy of proximity approximation as 5-10m scanning range raises false positives. • No real-time location information. • Higher programming requirements to ensure Bluetooth connectivity and response to App.
Bluetooth + UHF RFID	• Higher accuracy with double check. • Can track the belongings and items in use of the patient.	• Higher cost of tagging items and deploying RFID readers with RSSI and phase.
WiFi router tracing	• Widely available. • Wide range of different types of existing WiFi routers can be used with no extra hardware.	• Relatively low accuracy.
Mobile network tracing	• No App installation is required. • Transparent to the user. • Larger public access, who, if desired, could opt-out of the programme.	• List of devices that have made contact is not available. • Only high-level localisation information is available. • Participation of network operators is required to increase coverage.
UWB 5G	• High accuracy	• Not yet fully operational
Social media	• A pre-outbreak pattern can be identified predicting the next affected areas. • Could generate near-real-time information.	• Location and financial transactions information give rise to privacy issues.
Wearable devices using Bluetooth/ GPS/ WiFi	• Suitable for high traffic and dense areas including indoors, malls, homes. • Enables tracking & geofencing. • Increased coverage and reliability. • Cost effective.	• Requires a customized wearable device. • App has to run at all times. • Can generate false positives as range is higher than 1.5m.

What are the ethical issues and what steps should Scottish Government take to secure public trust?

(*Claudia Pagliari, Usher Institute, University of Edinburgh*)

Trust and ethics

Ensuring the health, safety and security of Scotland's people is critical as we face this global pandemic, yet doing so must not come at an unacceptable cost to their privacy or civil liberties.

While governments in countries such as China, South Korea and India have adopted a range of privacy-invasive and coercive approaches in their efforts to control the spread of COVID-19, many of these are unacceptable in Western democracies, where the desire for freedom from government surveillance and interference is strongly felt. In the case of contact tracing apps, this can be seen in the decisions of several European countries to move from centralised to decentralised approaches as a result of public unease, including Ireland and Germany[vii].

Debates surrounding the ethics of COVID-19 apps have chiefly concerned the extent to which they provide *anonymity* for individuals, *security* for their personal information, and protection for their *rights* as members of a fair and lawful society. Critical questions also relate to the *control* different actors hold over these technologies and the data they yield, which may potentially include not only public health authorities, but also other governmental agencies, third sector bodies, technology companies and others. The public's acceptance of *passive* digital health surveillance tools, such as thermal imaging cameras, their willingness to *actively* install and use mobile apps for proximity tracking or symptom reporting, and their comfort with different levels of *data sharing*, are influenced at least as much by their *trust* in these actors as in the technologies themselves.

These ethical issues can be further broken down into the entities requiring trust and the questions these provoke:

Key Dimensions of Trust and Ethics in Digital Contact Tracing Apps

The **technology** - Will it work reliably, is it safe, is it secure?

Its **privacy** policies - Does it use only the minimum necessary data, is consent required, how anonymous is it, will data be deleted after COVID-19?

Its **usefulness** – Is it needed for this purpose, does it achieve what it claims to, is the value worth the privacy trade?

The **people** developing it - Are they being transparent about the project's ambitions and scope, do they have secondary motives?

The **institutions** responsible for delivering it - Is there sufficient oversight and accountability; are there adequate processes and expectations for stakeholder involvement?

Its effects on citizens' **autonomy and rights** - Are people free to choose whether or not to use it, could it restrict their liberty or lead to discrimination?

Transparency and Accountability

Aside from the important issues of privacy/anonymity and protection from harm, coercion or discrimination, *transparency* and *accountability* are central prerequisites for ethical digital health.

Secretive and centralised decision-making by small groups can backfire, partly because it risks mistakes in design or functionality that could have been avoided with more experience at the table. For example, earlier release of the NHSX app's software code could have prevented embarrassing security glitches that later came to light.[viii] It can also leave observers in a state of *uncertainty* about the solutions being developed; leading to misunderstanding and speculation which may be reputationally damaging or disruptive.

Ethical concerns about "***mission creep***" have also been expressed. This concerns the possibility that technologies and data flows implemented for managing the pandemic may be re-used for other governmental purposes, such as policing, profiling or designing 'nudge' techniques, as well as for unspecified academic research or commercial innovation. During COVID-19 such concerns have been exacerbated by the participation of private-sector data-mining companies in the NHS response effort. Accusations of mission creep were levelled at NHSX, after plans were revealed to include an optional symptom reporting feature in its contact tracing app and harvest the data for future research.[ix]

As the above example shows, feelings can run high when digital initiatives are perceived as over-reaching their data needs and transparent, consistent ***public messaging*** is essential. Available information about the app proposed for the NHS in Scotland emphasises restricted use for official contact tracing and a privacy-respecting architecture that excludes proximity tracking, offering some reassurance for citizens worried about mass surveillance.[x] In parallel, however, medical researchers in Scotland have been encouraging citizens to download the semi-commercial Zoe app, which shares detailed personal data on symptoms, location, demographics and test results with the SAIL databank, where it can be linked with other data and accessed for research via the HDRUK Innovation Gateway.[xi] Nearly 3 million people across the UK have downloaded this app, which is now co-sponsored by the UK government and whose app store listing refers to the NHS, creating room for confusion. Given their very different implications for personal data, it will be important to establish how easily citizens can tell the difference between these 'NHS' apps.

Public engagement and involvement

Understanding citizens' needs and tolerances is also essential for digital projects and programmes. While previous research on public attitudes to digital health and big data is a useful guide, and there is a long literature on human behaviour during disease outbreaks, there is relatively evidence at the intersection between these two, and very little in the context of COVID-19 apps.

Various methods of public engagement exist, some more geared towards to *informing* citizens of new services, policies, risks or technologies, others towards *understanding* their needs, attitudes and concerns, and others aimed at *involving* them in decision-making or policy shaping. Challenges during a fast-moving outbreak are that some of these methods are time consuming or typically require physical meetings, although adaptations are possible, such as online surveys, telephone interviews, social media listening or remote dialogues/deliberations.[xii] , [xiii]

Just as a lack of access to technology, or ***digital exclusion[xiv],*** affects some people's ability to benefit from online services and apps during a pandemic, it also affects the way in which they can be informed, consulted, engaged, or involved in decision making. This is doubly problematic, since these are often the same elderly or vulnerable groups most at risk from COVID-19 and in need of support. Analogue methods, such as telephone surveys, radio or

television phone-ins, and paper-based questionnaires, are all possible ways to gather these citizens' views. In the present circumstances, however, engaging with community leaders and support groups as intermediaries may be more useful and effective.

Citizens' trust in digital contact tracing apps, and their willingness to use them also depends on how **useful** and **necessary** they believe them to be, which is likely to vary depending on the stage of the pandemic and the policies surrounding it (e.g. new outbreak, rapidly escalating deadly epidemic, lockdown, declining incidence and return to school/work). If the effort required to use an app, or the breadth of personal data it collects is seen as disproportionate to the stated need, then citizens will be far less inclined to use it.

Lessons from similar countries to Scotland

It is important to recognise that *even when the requirements for ethical use are largely satisfied app usage cannot be guaranteed*. Singapore - a democratic country with a population roughly the size of Scotland's - enjoys high levels of public trust in government, high compliance with laws, high levels of digital inclusion and its COVID-19 app 'TraceTogether' uses the decentralised Bluetooth proximity tracking model favoured by privacy professionals. Despite all of these factors, less than a quarter of the population has downloaded the app, due partly to privacy concerns but largely because the current version depletes mobile phone battery life. Apple's latest operating system update should address the latter problem, but it remains to be seen whether rates of uptake increase, particularly while the outbreak is largely confined to already-quarantined migrant workers, thus limiting its usefulness.[xv]

New Zealand's successful containment of COVID-19 has been partly attributed to public compliance with social distancing, enabled by high levels of trust in government. The country recently implemented a privacy-preserving approach involving optional QSR code scanning, rather than location or proximity tracking. However, concerns over proposals to integrate Bluetooth tracking and about the app's usefulness, mean that its future is uncertain.[xvi]

As these examples show, public trust in and acceptance of digital technologies like COVID-19 apps is dynamic and dependent on multiple factors. Engaging regularly and openly with citizens will be essential for understanding what is regarded as appropriate, necessary and proportionate under changing circumstances of risk and in different communities. Care should be taken to avoid mission creep or scenarios that unfairly benefit certain stakeholders, which could prompt accusations of '*data opportunism'*.[xvii] Importantly, consideration needs to be given to the necessity and likely benefits of any app, given the potential for wasted resources[xviii], since sustaining health and care services is also an ethical priority.

Discussion

The Scottish Government is having to make rapid and important decisions about how to respond digitally to COVID-19. These require carefully balancing respect for citizens' privacy with a desire to use technology and data to support disease surveillance, health service delivery, national statistics, research and innovation. Amongst these, apps that involve citizens as partners in contact-tracing efforts represent an immediate priority and one that has inspired both rapid global innovation and considerable debate.

This article illustrates how different *perspectives* influence the ways in which different communities of practice are approaching this challenge, with the computer scientist focusing on the privacy propositions offered by different proximity tracking models, the engineer analysing technologies and communication standards associated with contact tracing initiatives, the public health expert emphasising the benefits of capturing citizens' contacts and

symptom data for operational, analytical and clinical purposes, and the social scientist describing the ethical issues affecting the likely acceptance and uptake of these tools.

As these summaries show, there is no one 'perfect' solution for digital contact tracing and debate around their relative merits and risks is likely to continue.

What is clear is that, for Scotland to embrace its aspirations as an 'ethical digital nation[1]', further work is needed to find the optimum balance of privacy-respecting, secure, useful, inclusive and ethically acceptable innovations. This recognises the World Health Organisation's definition of health as a state of physical, mental and social wellbeing, not merely the absence of disease, including the protection of fundamental rights, social equality, an informed and participative public, and responsible governance.

Given the urgent needs presented by the current crisis, we recommend greater transparency and public engagement as well as further work to unpick the privacy, value and ethical challenges of alternative models. This needs to take account of both international experiences with these approaches, the changing risk context of COVID-19, and the unique needs of Scotland's health service, culture and communities.

Authors' caveat: At the time of writing (last update June 1st, 2020) only a sparse schematic for a digital contact tracing solution had been published by Scottish Government (drafted by DHI), which appears on the final page of the *Test, Trace, Isolate, Support* strategy document released on May 4th. The authors' contributions are therefore largely based on what is known about approaches elsewhere and on expert considerations of the optimal scenarios for public health, technology privacy/ security, and digital ethics.

References

[i] Tapper, J. (2020, April 4). *Recruit volunteer army to trace COVID-19 contacts now, urge top scientists*. The Guardian. http://www.theguardian.com/world/2020/apr/04/recruit-volunteer-army-to-trace-coronavirus-contacts-now-urge-top-scientists

[ii] Pagliari C, Vijaykymar S. Digital Participatory Disease Surveillance and the Zika Crisis. PLOS Emerging and Neglected Tropical Diseases, 13th June, 2016 https://inforrm.org/2020/05/02/coronavirus-contact-tracing-apps-a-proportionate-response-robin-mansell/

[iii] Cha V and Kim D. 2020. A Timeline of South Korea's Response to COVID-19. Centre for Strategic and International Studies. 18 March 2020. Available at: https://www.csis.org/analysis/timeline-south-koreas-response-covid-19

[iv] Lipsitch M, Swerdlow DL, Finelli L. Defining the Epidemiology of Covid-19 — Studies Needed. N Engl J Med [Internet]. 2020 Mar 26;382(13):1194–6.

[v] Wynants L, Van Calster B, Bonten MMJ, Collins GS, Debray TPA, De Vos M, et al. Prediction models for diagnosis and prognosis of covid-19 infection: systematic review and critical appraisal. BMJ 2020 Apr 7;369:m1328.

[vi] Buchanan, W. et al. Review and Critical Analysis of Privacy-preserving Infection Tracking and Contact Tracing. May 2020

[vii] Abboud L, Miller J, Espinoza J. How Europe splintered over contact tracing apps. Financial Times, May 10th 2020 https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10

[viii] Culnane C, Teague V. Security analysis of the NHS COVID-19 App StateofIT, May 19th, 2012 https://stateofit.com/UKContactTracing/

[ix] Lomas N. UK privacy and security experts warn over coronavirus app mission creep. TechCrunch April 29th, 2020 https://techcrunch.com/2020/04/29/uk-privacy-and-security-experts-warn-over-coronavirus-app-mission-creep/?ncid=txtlnkusaolp00000618

[x] Scottish Government. Coronavirus (COVID-19): test, trace, isolate, support strategy. May 4th, 2020 https://www.gov.scot/publications/coronavirus-covid-19-test-trace-isolate-support/pages/6/

[xi] Usher Institute. Statement on COVID-19 Symptom Tracker app. 7th April 2020.

[xii] NESTA. 3 Ideas for blending digital and deliberative democracy. 20th Feb, 2019 https://www.nesta.org.uk/blog/three-ideas-blending-digital-and-deliberative-democracy/

[xiii] Scottish Government. Coronavirus (COVID-19) conversation proves very popular. Digital Engagement Blog. https://blogs.gov.scot/digital-engagement/2020/05/08/coronavirus-covid-19-conversation-proves-very-popular/

[xiv] Disconnected. Understanding digital inclusion and improving access. Citizens Advice Scotland, Feb 2018 https://www.cas.org.uk/system/files/publications/cas_disconnected_report.pdf

[xv] Sim D. Why aren't Singapore residents using the TraceTogether contact tracing app? SCMP, May 18th 2020 https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether

[xvi] Harb R. New Zealand releases Bluetooth-free Covid-19 tracing app. The Register, May 20th, 2020 https://www.theregister.com/2020/05/20/new_zealand_scaled_back_digital/

[xvii] Mansell R. Coronavirus contact tracing apps: A proportionate response? https://inforrm.org/2020/05/02/coronavirus-contact-tracing-apps-a-proportionate-response-robin-mansell/

[xviii] Taylor J. How did the CovidSafe app go from being vital to almost irrelevant? Guardian, 23rd May, 2020 https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant