Scientists for Labour

COVID-19: Contact Tracing

Paul Henry,
Joe Eastwood,
Adam Thompson
Omar Salem,
Sam Fowles,
Ben Fernando

10/05/2020

Authors

Paul Henry is the Vice-Chair (Membership) of Scientists for Labour and a financial technology consultant specialising in data science and analytics. Prior to his current role Paul completed a PhD in biotechnology and machine learning at the University of Nottingham.

Joe Eastwood is an executive committee member of Scientists for Labour and a PhD student at the University of Nottingham specialising in machine learning and digital image processing for precision measurement.

Adam Thompson is the Vice-Chair (Policy) of Scientists for Labour and a research fellow in metrology at the University of Nottingham. Adam's role in Scientists for Labour is to coordinate and oversee policy development.

Omar Salem is a Vice-Chair of the Society of Labour Lawyers. He writes in a personal capacity.

Sam Fowles is a barrister at Cornerstone Barristers and a Fellow at the Foreign Policy Centre.

Ben Fernando is the Chair of Scientists for Labour and a postgraduate researcher at the University of Oxford.

Scientists for Labour

Scientists for Labour is a socialist society affiliated to the Labour Party. Our aims are to both promote good science in politics, and promote Labour values in science. More information about Scientists for Labour, including how to join, can be found at https://www.scientistsforlabour.org.uk. You can follow us on Twitter @scientists4lab.

Throughout the COVID-19 crisis, Scientists for Labour are preparing briefings and summaries of the latest research into coronavirus for Labour Party representatives and their staff. If you would like to receive these briefings or have any other queries, please contact Benjamin Fernando: chair@sfl.org.uk.

9th May 2020

Executive summary

In this report, Scientists for Labour investigate the potential of public health surveillance as a method to contain the spread of COVID-19 and provide greater insight into the spread of the disease. This work presents two fundamental questions which the authors believe must be answered by the UK Government prior fully implementing automated contact tracing across the nation:

1. **What steps will be taken to ensure that automated contact tracing is an effective tool for containing the spread of COVID-19?**
2. **How will the privacy of citizens be guaranteed?**

Automated contact tracing involves the collection of information about participants' interactions with other people. It is used as a way of quickly notifying people that they may have previously been exposed to someone who has since tested positive for the disease of interest. During the COVID-19 pandemic, different implementations of automated contact tracing have been suggested for use with smartphone devices which can track location, proximity to other people, or both.

An examination of the technology behind contact tracing apps, and their implementation in other nations has raised significant concerns about its efficacy as a tool for containing the spread of the virus. Implementations of a contact tracing app in Singapore do not yet appear to have been successful, as it has insufficient uptake by the population to effectively trace exposed individuals. The only implementation which appears to have been successful has been in China, however, this implementation required the use of draconian regulation of the Chinese people, including mandatory app download and enabling authorities to examine devices at will.

Automated contact tracing apps also highlight the balance which must be struck between an effective means of containing the spread of the virus, and the privacy of individuals. This balance has led to two divergent approaches: centralisation, which provides little privacy from authorities, and decentralisation, which may not provide sufficiently detailed information to public health authorities about the spread of the infection but offers fewer privacy issues.

The UK initially opted to develop a centralised implementation of an automated contact tracing app, trialled on the Isle of Wight. Early reports suggest that a second contact tracing app is now under development with the assistance of Apple and Google. The authors of this report have concerns about the efficacy of automated contact tracing apps, and their potential impacts on the privacy of users, therefore we recommend that both implementations should come under close scrutiny prior to general release in the UK.

1. Introduction

1.1 Background

COVID-19 is the disease resulting from infection with SARS-CoV-2, a type of coronavirus. This virus first came to the attention of Chinese authorities in early January 2020, and in the resulting four months has rapidly spread across the planet, resulting in a global pandemic. Rapid human-to-human transmission and a high mortality rate have led to many nations adopting stringent policies to slow or prevent further spread of the virus. In the UK, these measures included a nationwide adoption of 'social isolation' measures, wherein the majority of the population has been instructed not to leave their homes aside from in specific circumstances. These measures have been enacted to prevent the National Health Service (NHS) critical care capacity being overwhelmed, which could lead to high rates of preventable deaths. However, such a restrictive regime will not be sustainable for long periods of time due to the adverse impacts it could have on the psychological health of the population and the national economy [1].

An appropriate method for lifting the lockdown has become a key issue of debate in recent weeks. As of 9am on 7 May, 1,534,533 COVID-19 tests have been carried out in the UK [2]. Whilst this number represents a significant operational effort, it does not provide sufficient visibility over the spread and transmission rate of the disease in the UK [3]. Without a greater understanding of the transmission rate and the geographical spread, it is impossible to make the decision to ease social distancing without putting the country at significant risk of a second, potentially more damaging wave [4]**.** As such, the level of testing in the UK has become a political issue, leading to significant criticism of the Government in national and local media [5].

Whilst the UK is ramping up its testing efforts, there has also been work on producing a **contact tracing application** (app), to help target testing and social distancing more effectively [6]**.** Such a large-scale public health surveillance operation could enable the country to exit the current lockdown, and quickly identify and prevent new outbreaks. However, health surveillance, especially that which captures extensive information on the geographical location (via GPS) and personal contacts of individuals should be used with extreme care, as such surveillance could easily infringe upon rights to privacy and autonomy.

1.2 Public health surveillance

Public health surveillance can be understood as, "the ongoing, systematic collection, analysis and interpretation of health data essential to the planning, implementation, and evaluation of public health practice, closely integrated with the timely dissemination of [this information] to those who need to know" [7]. Manual public health surveillance has been carried out in some form since the first recorded epidemic in 3180 B.C., with the modern concepts of health surveillance being founded by William Farr in the 1800s [8].

In 2012, Public Health England (PHE) outlined their vision for administering public health surveillance in "*Towards a public health surveillance strategy for England"* [7]. However, the context of the COVID-19 pandemic has dramatically changed the needs of any health surveillance system, with much of the emphasis now placed on tracking the spread of the disease. In this document, PHE describe public health surveillance as "**a core public health function that ensures the right information is available at the right time and in the right place to inform public health decisions and actions**", for the purpose of "[informing] **public health action, programme planning and evaluation, and formulating research hypotheses**".

Recent advances in mobile telecommunications, WiFi, and Bluetooth have enabled new approaches to capturing data that were not previously available. Geographical data from mobile phones can be used to predict sites of new outbreaks during an epidemic [9]. Additionally, big data analysis (i.e. computational analysis of extremely large datasets to reveal patterns, trends, and associations) was investigated as a route to helping contain the 2014-16 Ebola crisis in western Africa [10].

2. Contact tracing

2.1 Introduction

Contact tracing typically follows a three-step process, which is presented here and visualised in figure 1:

1. An individual tests positive for the infection of interest
2. That individual's potentially exposed contacts are identified – the definition of a potentially exposed contact will vary depending on the mode of infection of the disease
3. Identified contacts are notified, invited for a test, and informed on how best to prevent further transmission

During the current pandemic, contact tracing has been used in some nations as an effective form of public health surveillance, particularly during the early stages of the outbreak in South Korea. Using these methods, potentially infected individuals are identified and isolated if they have had recent contact with someone who has contracted the disease.

2.2 Past usage

There is a precedent for contact tracing methods being utilised to mitigate the effects of global pandemics. Notably, throughout the ongoing global HIV global epidemic, contact tracing has been used in many nations to identify sexual partners and other potentially exposed acquaintances of infected individuals. This approach has enabled authorities to better understand the spread of the disease, contributing to research and public health decision making, as well as enabling potentially infected contacts to get tested and take steps to prevent further transmission [11].

However, whilst manual contact tracing has been effective in the past for sexually transmitted infections such as HIV (with infected individuals reporting sexual contacts, for example), COVID-19 appears to be primarily spread through the inhalation of respiratory droplets [12]. Therefore, one individual could infect numerous others regardless of their social connection.

2.3 Methodology

For contact tracing to be effective in the current pandemic, it will likely be necessary to have access to information on the geographical location of individuals and the details of anyone who may have been in close proximity to them. This requirement has raised significant concerns over potential infringement on personal privacy and around how a practical implementation of geographical tracking could be done. Reviews of public health surveillance make it clear that these methods can only be effective so long as public trust is maintained [13]. In a 2020 article by Ienca and Vayena they make clear, "data collection must (i) be proportional to the seriousness of the public-health threat, (ii) be limited to what is necessary to achieve a specific public-health objective, and (iii) be scientifically justified" and that "overriding consent and privacy rights in the name of disease surveillance may fuel distrust and ultimately turn out to be disadvantageous" [14] .

It should also be noted that the COVID-19 situation is further complicated by the presence of **asymptomatic carriers**, who may not report themselves as infected, through no fault of their own. As

such, manual tracing of social contacts will be likely insufficient to detect all potential infections in nations where there is already a significant level of infection [15].

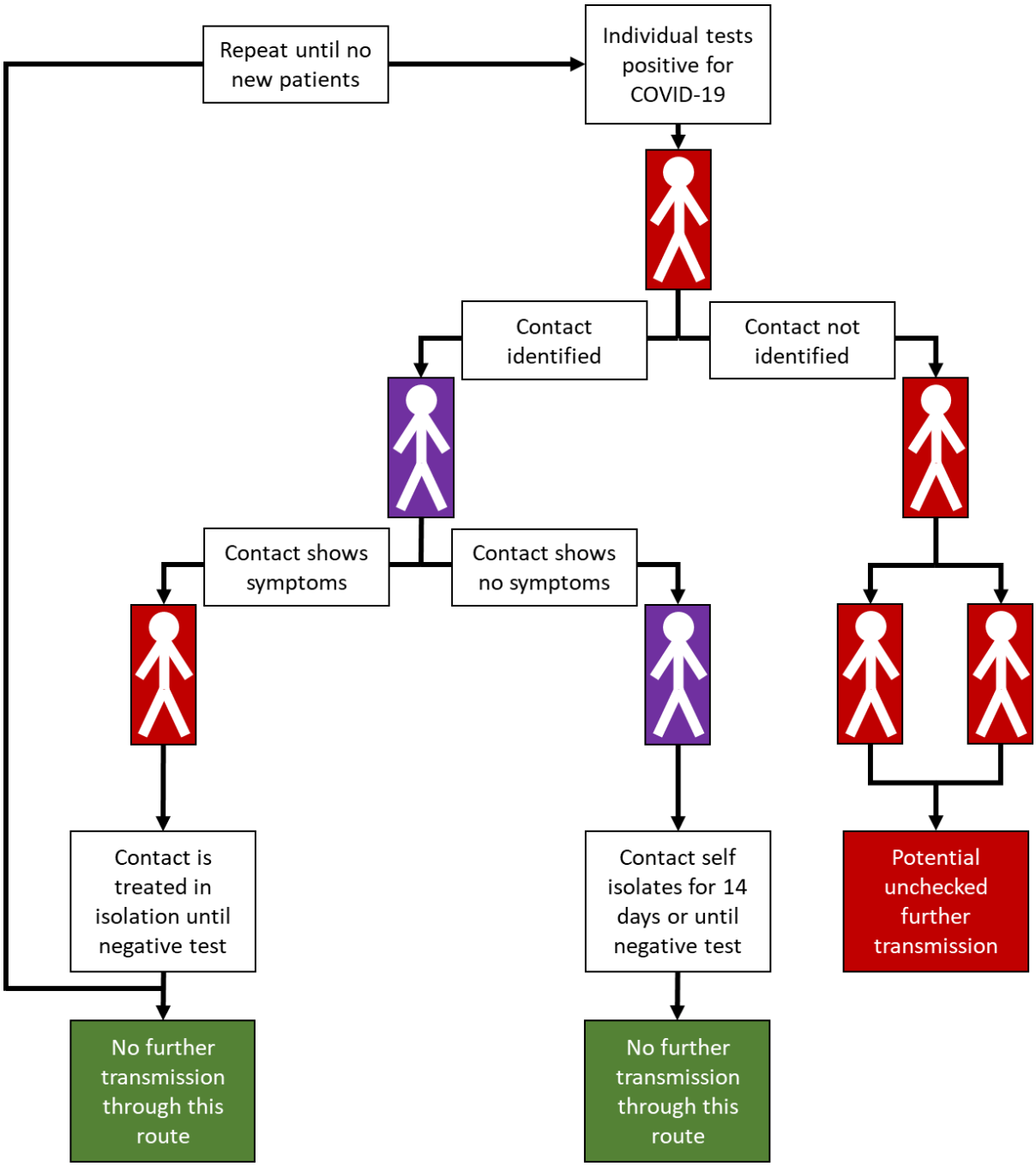

Figure 1: Contact tracing flow diagram. Based on [16].

As manual contact tracing is unlikely to have sufficient capacity to track the rapid spread of COVID-19, automated alternative solutions have been proposed. To overcome the limitations of manual contact tracing methods, many nations and private enterprises have conceived mobile phone applications (apps) which could be used as automated alternatives to manual contact tracing. Many of the proposed solutions will collect information on the precise location and proximity to other individuals with the app for all users. When an individual contracts the virus this information can be rapidly accessed, allowing notification and advice to be sent out to everyone who may have been exposed to the virus. Solutions combining location and proximity data will likely have to continually collect information on users for the duration of time that the app is downloaded on the device. In many app

implementations, while the contact tracing app is active, Bluetooth can be used to exchange information between users which come within a specified proximity of one another and location information is gathered using existing GPS functionalities [6].

The collection of such detailed information could additionally be used to inform the models investigating the spread of the virus, giving political decision makers much greater insight into the efficacy of other interventions, such as social isolation [17]. However, for digital contact tracing to be an effective method for measuring the dynamics of a disease outbreak and notifying potentially infected people, it requires a significant uptake across the population [18]. Concerns about the efficacy of contact tracing raises key questions as to whether it is an appropriate response, as the collection of such sensitive personal information could also constitute a significant breach of privacy.

2.4 Efficacy

In an attempt to reduce the spread of COVID-19 in line with the policies of many other nations, the UK has been practicing widespread social isolation for all but "essential workers". Whilst this policy appears to have prevented NHS critical care capacity from becoming overwhelmed, it has caused significant economic and social damage. Many people have been placed on the Government furlough scheme, and there has been a considerable rise in incidences of domestic violence [19]. Aside from these immediate impacts, worldwide lockdown is also expected to contribute to a global economic recession [20]. With such dire consequences, understandably many national governments are seeking an effective strategy for exiting the lockdown without triggering a second, potentially more damaging outbreak. Contact tracing is part of the UK *test, track and trace* strategy for the next phase of the pandemic. A successful contract tracing app could enable the rapid identification and isolation of infected individuals, resulting in a lower effective rate of transmission, as well as allowing the Government to target policies to aid impacted local areas [21].

However, successful implementation of an automated contact tracing app will be challenging for two key reasons:

1. Effective surveillance of the population and timely notifications to infected individuals will rely upon a high level of uptake of the app.
2. The contact tracing process is triggered by confirmation of infection, which requires an accompanying programme of mass testing.

Depending on their complexity, mobile phone apps can be time consuming to develop, though a number of apps have already been released and more still announced (see sections 3 and 4, respectively). I**n the case of an automated contact tracing app, there are many relevant development considerations, such as the ability to collect GPS data, operating in-built Bluetooth functionality, and compatibility with both Android and Apple operating systems** [22]. Aside from the expense and complexity of app development, the impacts on users' devices must also be considered. Real-time data collection could come at significant cost to the individual (depending on their personal service provider), and constantly using GPS and Bluetooth functionality could become a significant drain on device battery usage [23].

Another key issue facing the use of automated contact tracing apps is **ensuring a high enough uptake** for the app to be generally fit for purpose. At present, the UK Government suggests a target uptake of 80 % of smartphone users for its purpose to be fulfilled [24]. The most downloaded smartphone apps are typically messaging and social media services – WhatsApp, for example, has a reach of around 58 % of mobile messaging users in the UK [25]. **To ensure high uptake of a contact tracing app, a significant advertising campaign and incentivisation programme may be required**. In Singapore,

roughly a quarter of the population have downloaded the TraceTogether app, giving a 6 % chance of any two randomly selected people coming in contact both having the app [26].

Even with incentives, it is unclear how many people would be in a position to use the app; battery-life and data considerations may put some users off, while others may have an older device which is not capable of supporting the software. Whilst smartphones have become increasingly common over the last decade, there is still a **significant drop in their usage amongst the over 55s** in the UK, compared to younger demographics [27]. Given that older populations are most at risk from the effects of COVID-19, uptake may not be high enough amongst the most at-risk demographics for a contact tracing app to be of significant value.

The efficacy of a contact tracing app will likely rely on the app being paired with regular and thorough testing of the population, both to gather information on the spread of the disease, and to notify individuals of potential transmission. Therefore, contact tracing is additionally unlikely to be effective without a significant mass testing effort [28].

2.5 Privacy

There are three key considerations for contact tracing apps with regards to privacy: p**rivacy from snoopers; privacy from contacts; and privacy from the authorities** [29].

In these considerations, snoopers are individuals accessing the publicly available data being broadcast by the apps. For example, **snoopers** may sit in a public place, simply observing the tokens, pieces of information which stand in for personal identities, of people walking past, from which they can directly read or infer private information. Such snooping often takes the form of 'linkage attacks', where a user's real identity is deanonymised by linking them to a digital ID. The real identity of the individual can then be used for malicious purposes, such as publicly revealing sensitive personal information.

Privacy from contacts involves insuring that sensitive personal information is not shared accidently or intentionally between social groups and clusters. Such sharing may include revealing the identity of infected people to their entire residential area. **Privacy from authorities**, such as private enterprises administering the app or the central government, is determined by the what data is collected, with whom it is shared, and how it can be used for purposes other than contact tracing.

Following the global surveillance network revealed by the whistleblower Edward Snowden in 2013, the transfer of citizens information to security services has become a significant privacy concern [30]. These disclosures showed that security services in the USA, UK, Canada, Australia and New Zealand were spying on the internet communications of their own citizens, as well as on foreign nationals. The disclosed files also contained information on commercial partners such as BT, Google and Facebook, who provided access to the private information of their users [31]. Despite global outrage, the collection and centralisation of personal data has intensified, particularly in the case of private companies such as Google and Facebook, who rely on a targeted advertising business model [32]. The implementation of a contact tracing app which collects information about its users' movements and interactions could, therefore, present a significant risk to individuals' privacy from authority.

Besides the issues surrounding infringement on personal liberty that these apps may impose, if an app is viewed to be untrustworthy or too invasive, it is likely, especially in Western nations where governments are less likely to mandate app usage, that the public will simply not use or install such an app. As these apps will only be effective if there is significant uptake, insufficient privacy protections are likely to become self-defeating.

2.6 Centralised versus decentralised

Two competing approaches have emerged in the development of contact tracing applications, so called **centralised and decentralised**. In a centralised system, when two devices running the app detect each other via Bluetooth they swap tokens. These **tokens**, or user IDs, use a technique called hashing to produce a unique message which cannot be reversed. Periodically all devices running the app upload the list of tokens they have collected to a **central server**. When a user identifies themselves as infected, the server scans the database of tokens and informs all users who have collected the infected person's token that they are at risk. This means that all data of interest to the device, be that user IDs, location, connections, and matches – are all collected and stored on this central server.

Similarly, a decentralised approach also works through devices exchanging tokens. However, in this case they do not upload these tokens to a central server. Instead, when a person marks themselves as infected – they alone upload *their own* tokens (as opposed to the list of tokens referring to other individuals they have collected). Periodically all users download the list of infected device tokens to their own device and check their own set of collected tokens against it to see if they are at risk. In contrast to the centralised approach, no information is stored centrally about non-infected users, and the 'matching' process which determines who is at risk is done locally on the user's device instead of on the central server. In this way, the central server also has no information about the contacts between devices.

Even if a user's data is fully anonymised, a much larger proportion of this data is captured and stored by the central authority running the app in the centralised case. This may make it easier to perform linkage attacks to de-anonymise the data but may also improve the efficacy of the app in providing useful information to help prevent the spread of the virus. This is a clear demonstration of the balancing act between efficacy and privacy which is at the heart of this problem.

Any centralised system of contact tracing will necessitate some capture of information from its users, creating an **inevitable trade-off between efficacy and privacy**. A centralised implementation would collect and store information on their users in a central database, owned and maintained by either a private company or national government. In such a system, a record of the movements and interactions of users, coupled with widespread testing, could provide valuable information about the spread and dynamics of the COVID-19 pandemic. However, the only protection from secondary usage for security or enterprise purposes would be strict controls on which agencies had access and legal frameworks regarding the deletion of data after a set timeframe.

A decentralised system still relies upon exchanging tokens when mobile devices come within proximity of one another. However, these are not immediately uploaded to a database as in the case of centralised implementations. When a user receives a positive test result for the virus they upload the tokens which refer to themselves to a cloud database. All users periodically download this database of tokens representing infected people, so the cross-referencing of people that they have come into contact with and those who have become infected can happen on their own devices, rather than being performed by a government agency or private company. This system ideally ensures that records of interpersonal interactions only exist on individual's devices, ensuring privacy from authority. To improve privacy from snoopers, individual tokens can be regularly changed by the app, so when the user is infected they upload a series of tokens rather than a single one which may be linked to their identity. A visualisation of the difference between centralised and decentralised app implementation is presented in figure 2.

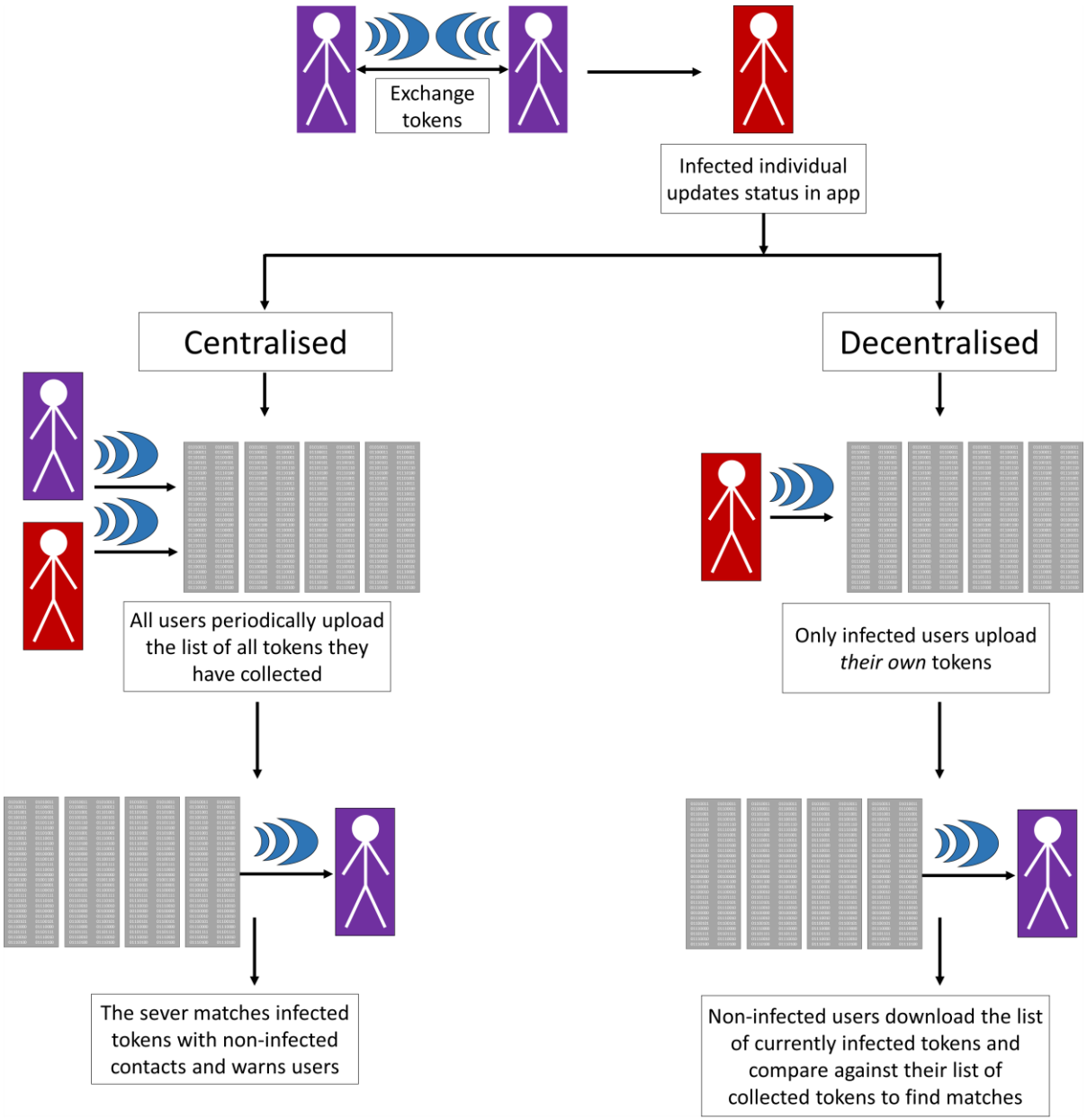

Figure 2: Decentralised vs centralised app implementations. Based on [55].

Some contact tracing implementations, such as Singapore's **TraceTogether**, attempt to overcome some of the concerns around privacy from authority by eschewing GPS data completely and relying solely on Bluetooth interaction information [33]. Some of these Bluetooth-only apps have been shown to comply with various privacy standards [34]. However, systems wholly reliant on this interaction data are limited as they are unable to model disease transmission from commonly contacted surfaces [35]. Bluetooth-only system will require specially designed apps, and will likely be a significant drain on device battery life, whereas GPS data is already collected by a number of apps, such as Google maps, potentially enabling contact tracing to be a plugin for existing apps.

Another potential route to improving the privacy of apps is the use of cryptographic approaches, which would encode information so that potentially impacted people could be notified without resorting to mass surveillance. With such an implementation, accurate GPS and Bluetooth interaction data could be collected and encrypted so snoopers and authorities would be unable to read it. The use of cryptography would see a significant increase in the computational cost incurred by the app and would present a trade-off between privacy and efficiency [36]. This implementation still places trust in the

government to use a secure hashing algorithm, which irreversibly converts information into an unintelligible numeric string. However, there is historical precedent showing that such trust can be unwarranted, such as the exploits found in the secure hashing algorithm (SHA1) developed by the NSA.

There are significant and reasonable concerns about the impact contact tracing apps could have on individual privacy, which must be addressed by any implementation. Methodologies which could be used to maintain user privacy often come with associated costs, such as efficacy, efficiency and individual device performance, creating situations where the needs of individuals, communities and public health authorities must be carefully considered and balanced. Public trust could be gained by open sourcing app details (i.e. freely distributing the app with its source code available for modification) and allowing audit by independent security and privacy professionals. Open sourcing would enable users to know exactly what data is being taken, who can access that data and for what purposes it is being accessed [29].

2.7 Data anonymisation

A note is provided here on **data anonymisation**. Anonymisation is a process which irreversibly alters data so that an individual cannot be identified directly or indirectly [37]**.** However, it should be noted that anonymisation is not a fixed state where individual privacy is totally protected; anonymisation often strikes a balance between analytical utility and privacy. Deanonymisation attacks have been reported for a variety of data sources; identifying individual locations, financial activities and preferences [38].

3. Current app implementations

There have been several implementations of contact tracing apps attempted across the world since the outbreak of COVID-19. Examples of various implementations internationally are as follows [29]:

- The Israeli state passed a law allowing the mobile phone data of infected individuals to be tracked directly;
- The South Korean government has developed a database containing the age, gender, travel routes, and occupations of infected individuals;
- Taiwan allow medical institutions to access to the travel history of infected patients and the state to track the phones of individuals placed into quarantine;
- Singapore have released a centralised app called TraceTogether; and
- China have mandated use of a centralised app called Alipay Health Code.

3.1 Singapore

Singapore first detected cases of COVID-19 in late January, immediately beginning manual contact tracing in an effort to contain the spread of the infection. On the 8th February, the Singaporean Prime Minister stated that it was “futile to try to trace every contact” [39]. By mid-March, Singapore launched the world’s first COVID-19 contact tracing app, TraceTogether, alongside a swathe of other policy measures focused on socially distancing the population. The TraceTogether app was developed to maintain high levels of privacy from snoopers and contacts. Tokens exchanged through Bluetooth proximity were associated with a user ID which changed with time, making it considerably more impractical to launch linkage attacks. Privacy from contacts has been strengthened by solely notifying contacts of a potential exposure, rather than providing details of the infected person, or when the exposure may have taken place. However, the TraceTogether app currently provides little privacy from authorities, as infected individuals and potentially exposed contacts automatically have their phone numbers collected by the state [29]**.**

The TraceTogether app claimed to have over 1.4 million users as of 5 May, which accounts for a quarter of the population of Singapore, so the chance of two random people coming into proximity with one another and both having the app is around 6 %. A significant complaint of the app is that it cannot be run in the background on iPhones, as Apple does not permit background apps to use Bluetooth for security reasons. TraceTogether users with iPhones are required to keep the app running at all times, which drains device power and can interfere with other processes [40]. In May, the Singaporean government also announced that all businesses would be required to log the presence of visitors, by collecting a national identity number and the time of entry and exit of the premises by scanning people's phones using another app called SafeEntry. This new app will be compulsory for all businesses and citizens entering public venues [41]. This measure may be due to the relatively low uptake of the contact tracing app, or the limitations of the current, Bluetooth-only, implementation. The Singaporean government has stated that the data collected by the app may only be used "by authorised personnel for contact tracing purposes", and that "stringent measures are in place to safeguard the data in accordance with the Government's data security standards" [42].

3.2 China

In China, a contact tracing app called AliPay Health Code has been implemented through the almost-ubiquitous digital service providers AliPay and WeChat. This implementation provides a colour-coded digital health pass which can be checked by authorities to ensure efficacy of the lockdown. This app collects travel, contact and biometric information to rate each user as green, yellow or red, which, in turn, dictates whether any one individual is allowed to be in public spaces [43]. The app has come under significant criticism from privacy campaigners due to the vast amounts of personal data it collects, and for the presence of a function in the source code, labelled "reportInfoAndLocationToPolice"; which sends individual names, locations, city name and an identifying code number to another server [43]. Whilst the Chinese government appear to have discovered an effective route to containing the pandemic, this has in part been through further erosion of individual privacy from authorities [44].

Both the Singaporean and Chinese experiences with contact tracing demonstrate the challenges faced when tracking and containing the spread of COVID-19. For many nations manual contact tracing will not be practical or effective, as the number of infections is likely too large, and the respiratory transmission of the virus will make it unlikely that a single infected individual would personally know everyone they may have exposed. Whilst automated contact tracing apps could potentially overcome these issues, they will likely require some infringement of individual privacy, and without a strict legal incentive are not guaranteed to have sufficient uptake to be effective.

4. Future implementations

It was recently announced that Apple and Google were working together to create a standard Application Programming Interface (API), upon which contact tracing apps could be built. This proposed solution would take a decentralised approach, bypassing the requirement for individual location or interaction data to be collected and stored by any single Government or private entity [45]. Each user will be assigned a regularly-changing unique identifier (an ID), with the IDs of only users who test positive for COVID-19 being added to a cloud database. When two people come into contact, they exchange these user IDs, hashed with the current time, with each device regularly scanning the cloud database for COVID-19 positive IDs. Using this implementation, the records of those who have been in contact with one another are maintained on each individual device, where the matching process takes place. This approach provides much greater privacy from authority than a centralised approach. However, depending on the security and how user IDs are exchanged it could raise issues relating to privacy from snoopers or contacts. Such privacy breaches are likely due to the considerations noted above, but edge cases are possible (for example, if a person receives a notification after visiting a single individual). One of the major benefits of this implementation could be its effect on battery life,

as Google and Apple manage the two most prevalent mobile device operating systems, potentially allowing them to develop a system which best takes advantage of existing functionality.

Whilst a decentralised approach offers much greater privacy from authority, it is unlikely to offer the same level of information to public health bodies than that of a centralised implementation. It should also be noted that in the past both Apple and Google have received criticism for infringing personal privacy [46]. Google have particularly come under fire for their unclear privacy policies and collection of extensive sensitive personal information with its maps, email and browser services [47].

5. Proposed approach in the UK

The government-run unit for developing digital healthcare innovation best practice and policy, **NHSX**, has been at the forefront of independently creating a contact tracing mobile app. This app began its first trial on the Isle of Wight on 5 May [48]. In April 2020, NHSX chose to abandon plans to codevelop the app with Google and Apple, and adopt a centralised approach in conjunction with the private companies Faculty and Palantir, with GCHQ in an advisory role [45,49]. The app will be based on a central database which will collect Bluetooth tokens from other users encountered by the device and allow individuals to register their infection, notifying all contacts to self-isolate and get tested. The development of the app has attracted significant criticism from privacy advocacy groups due to its use of a centralised database containing personal information, and the participation of Palantir and Faculty [50].

Palantir Technologies is a USA-based big data analytics firm which works with American defence agencies, financial institutions and healthcare providers. Previously, Palantir has been involved in a variety of well publicised controversies, including the 2018 Cambridge Analytica scandal [51]. Likewise, the involvement of the British firm, Faculty, has been controversial due to the connection with the Conservative Party and the Vote Leave campaign. The firm's CEO, Marc Warner, is the brother of Ben, a Downing Street advisor and attendee at the Scientific Advisory Group for Emergencies (SAGE) throughout the early stages of the COVID-19 crisis [52]. The involvement of a government intelligence agency such as GCHQ (at any level) may also raise public concern.

Aside from the chosen partnerships, the NHSX implementation has also come under fire due to its rejection of the joint Apple/Google approach. Due to security restrictions built into both the Apple and Android operating systems, the NHSX app will be unable to broadcast its ID to surrounding phones unless it is operating in the foreground of an unlocked device [53]. Under these conditions, the app will most likely be ineffective for collecting sufficient information for contact tracing. NHSX claims to have corrected the problem by developing a functionality which will 'wake' the app whenever another device running the app is within range, however, this function could have significant impacts on battery life. It should also be noted that the centralised approach taken by the NHSX is out of step with other approaches being taken across most of Europe – with the exception of France, other European nations are generally supporting the decentralised Apple/Google implementation [54].

The UK implementation of an automated contact tracing will be an opt-in system, with the NHS planning a significant accompanying marketing campaign. Studies have suggested that 80 % of UK smartphone users, which translates to 56 % of the overall population, will be required to download the app for effective suppression of the pandemic [18]. **With issues surrounding privacy and the impact of the app on personal device performance, attaining such a high uptake does not appear likely**.

The contact tracing app developed by NHSX has been trialled on the Isle of Wight from the 4th of May. Testing by the BBC found that the concern about the app not working in the background on iOS had been overcome and that the app seemed to work well even when not active [55].

We stated earlier in this document that a key to garnering public trust would be open and honest access to the inner workings of the app. To attend to the this, NHSX has published the source code of the app to GitHub which is certainly a step in the right direction [56].

The Joint Committee on Human Rights expressed concerns over the centralised approach, citing the possibility of de-anonymising the data. The chair, Harriet Harman said, "*Assurances from ministers about privacy are not enough. There must be robust legal protection for individuals about what that data will be used for, who will have access to it, and how it will be safeguarded from hacking*." There is now a possibility that due to these concerns, the NHSX app may be changed to run on the Google-Apple API. NHSX have hired a swiss consultant, Zühlke Engineering, to perform a two-week study into how the two approaches can be integrated. It is unclear at this stage whether the switch will be made, but initial reactions from privacy experts believe it would be beneficial [57].

5.1. Legal considerations

The Data Protection Impact Assessment (DPIA) for the app that NHSX is trialling on the Isle of Wight has recently been published and is being reviewed by the Information Commissioner's Office [58]. The DPIA should set out how, and on what legal basis, personal data collected is used by the app. It is important that the DPIA be subject to detailed and careful scrutiny to ensure that the app's use of personal data is lawful.[59,60] Personal data must be processed in accordance with the General Data Protection Regulation and the Data Protection (GDPR) Act 2018 [61]. Here, personal data is as defined by the GDPR (i.e. "any information which are related to an identified or identifiable natural person"). An additional concern is that, even where the data is considered personal, the protections of the GDPR and the Data Protection Act 2018 are insufficient. Parliament's Joint Committee on Human Rights has drafted a bill aimed at ensuring appropriate legal safeguards for personal data used by the app are in place.

6. Discussion & conclusions

With many nations attempting to navigate a path out of lockdown and to prevent further economic and social damage, public health surveillance through automated contact tracing has been proposed as a potential method for rapidly identifying and quarantining infected individuals. By tracking the location and interactions of individuals, the spread and dynamics of COVID-19 could be accurately identified, allowing for targeted interventions without mandating strict social isolation for the entire population. However, these apps will always present an imperfect solution will necessarily balance efficacy with individual privacy and device performance. A number of notable concerns have been raised in this report regarding the efficacy of any implementation of a contact tracing app.

The UK had initially decided to adopt an independent approach to the development of a contact tracing app, which will use a centralised database of user IDs. These choices raise significant questions regarding individual privacy and whether sufficient people will download the app to ensure it presents an effective method for containing the pandemic.

At the time of writing there are reports of a second app under development with the assistance of Google and Apple. Due to the requirements from both companies that a decentralised approach is adopted, this second app could provide greater protections to individual privacy and will likely coordinate more effectively with existing device systems.

Whilst the adoption of a decentralised system would be a welcome development, it is still of paramount importance that the app is thoroughly scrutinised in terms of its efficacy, impacts on privacy, and the role of private companies in its development and administration. Regardless of the technological approach taken by the government, there are still significant concerns regarding

whether any app will have sufficient uptake to effectively track the virus. If automated contact tracing is included in the UK lockdown exit strategy, the Government should provide a strong justification around why they believe that this implementation will be successful where others have so far failed.

7. Key Questions

An examination of the underpinning technology, choices of the UK Government and the implementations of other nations poses two key key questions regarding contact tracing:

1. What steps will be taken to ensure that automated contact tracing is an effective tool for containing the spread of COVID-19?
2. How will the privacy of citizens be guaranteed?

Further to these primary questions, answers to several supplementary questions are required. These questions include, but are not limited to, the following:
Sa

1. Given lower technological literacy (and hence likely uptake) and high risk from COVID-19 in older populations, how will effective contact tracing be implemented for those most at risk?
2. Will people identified as potentially exposed contacts be mandated to self-isolate? If so, how will this be practically enforced?
3. Under what conditions will contact tracing be discontinued?
4. Following the discontinuation of contact tracing will personal data be deleted?
5. For what length of time will data be stored after each recorded interaction?
6. How will personal data be stored and who will have access to it?
7. Who will have authority over the governance of which data is collected and who can access it?
8. Which third parties (both non-health related governmental agencies and private companies) will have access to the information collected by the app?
9. Will the contact tracing technology be made open source?
10.

It should be noted that this list of questions is not exhaustive, and other questions may present themselves to readers of this report. With these questions, the authors of this report hope to stimulate political discussion and ensure that citizens of the UK and the world both benefit from and remain protected through any potential implementation of contact tracing.

References

1. Anderson, R. M., Heesterbeek, H., Klinkenberg, D. & Hollingsworth, T. D. How will country-based mitigation measures influence the course of the COVID-19 epidemic? *The Lancet* **395**, 931–934 (2020).
2. UK Government. Number of coronavirus (COVID-19) cases and risk in the UK. (2020). Available at: https://www.gov.uk/guidance/coronavirus-covid-19-information-for-the-public. (Accessed: 8th May 2020)
3. Kemp-Benedict, E. *Macroeconomic impacts of the public health response to COVID-19*. (2020).
4. Rousseau, H.-P. Planning for a CUM-COVID rather than a POST-COVID society at a Major Canadian Socio-Economic Summit. *CIRANO Pap.* (2020).
5. Financial Times. How testing fiasco exposed Britain's flawed virus response. *Financial Times* (2020).
6. Guttal, V., Krishna, S. & Siddharthan, R. Risk assessment via layered mobile contact tracing for epidemiological intervention. *medRxiv* 2020.04.26.20080648 (2020). doi:10.1101/2020.04.26.20080648
7. Thacker, S. B. & Berkelman, R. L. Public health surveillance in the United States. *Epidemiol. Rev.* **10**, 164–190 (1988).
8. Langmuir, A. D. William Farr: Founder of Modern Concepts of Surveillance. *Int. J. Epidemiol.* **5**, 13–18 (1976).
9. Bengtsson, L. *et al.* Using mobile phone data to predict the spatial spread of cholera. *nature.com*
10. Bates, M. Tracking Disease: Digital Epidemiology Offers New Promise in Predicting Outbreaks. *IEEE Pulse* **8**, 18–22 (2017).
11. Adler, M. W. & Johnson, A. M. Contact tracing for HIV infection. *Br. Med. J. (Clin. Res. Ed).* **296**, 1420–1421 (1988).
12. World Health Organization. Modes of transmission of virus causing COVID-19: implications for IPC precaution recommendations. (2020). Available at: https://www.who.int/news-room/commentaries/detail/modes-of-transmission-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations. (Accessed: 8th May 2020)
13. Groseclose, S. L. & Buckeridge, D. L. Public Health Surveillance Systems: Recent Advances in Their Use and Evaluation. *Annu. Rev. Public Health* **38**, 57–79 (2017).
14. Ienca, M., medicine, E. V.-N. & 2020, undefined. On the responsible use of digital data to tackle the COVID-19 pandemic. *nature.com*
15. Ferretti, L., Wymant, C., Kendall, M., … L. Z.- & 2020, undefined. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *science.sciencemag.org* eabb6936 (2020). doi:10.1126/science.abb6936
16. Centers for Disease Control. *What is Contact Tracing*. (2016).
17. Information Commissioner's Office. *COVID-19 Contact tracing: data protection expectations on app development*. (2020).
18. Hinch, R. *et al.* Effective Configurations of a Digital Contact Tracing App: A report to NHSX. 1–29 (2020).
19. Mark Townsend. Revealed: surge in domestic violence during Covid-19 crisis. *The Guardian*
20. Chris Giles. BoE warns UK set to enter worst recession for 300 years. *The Financial Times* (2020).
21. UK Government. Coronavirus test, track and trace plan launched on Isle of Wight. (2020). Available at: https://www.gov.uk/government/news/coronavirus-test-track-and-trace-plan-launched-on-isle-of-wight. (Accessed: 8th May 2020)
22. Vincent, J. Without Apple and Google, the UK's contact-tracing app is in trouble - The Verge. *The Verge* (2020). Available at: https://www.theverge.com/2020/5/5/21248288/uk-covid-19-contact-tracing-app-bluetooth-restrictions-apple-google. (Accessed: 8th May 2020)
23. Bradshaw, T. & Warrell, H. How the UK's unique coronavirus contact tracing app works. *The*

Financial Times (2020).
24. Kelion, L. Coronavirus: NHS contact tracing app to target 80% of smartphone users. *BBC News* (2020). Available at: https://www.bbc.co.uk/news/technology-52294896. (Accessed: 8th May 2020)
25. Bucher, B. WhatsApp has grown its user base by 20% in UK. *Messenger People* (2020). Available at: https://www.messengerpeople.com/whatsapp-user-base-uk/. (Accessed: 8th May 2020)
26. Nature. Show evidence that apps for COVID-19 contact-tracing are secure and effective. *Nature* **580**, 563 (2020).
27. Boyle, M. Mobile internet statistics 2019. *Finder UK* Available at: https://www.finder.com/uk/mobile-internet-statistics. (Accessed: 8th May 2020)
28. Kim, H. & Paul, A. Contact Tracing: a game of big numbers in the time of COVID-19. (2020).
29. Cho, H., Ippolito, D. & Yu, Y. W. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. (2020).
30. Halbert, D. & Larsson, S. By Policy or Design? Privacy in the US in a Post-Snowden World. *J. Law, Technol. Public Policy* **1**, 1–17 (2015).
31. Bauman, Z. *et al.* After Snowden: Rethinking the Impact of Surveillance. *Int. Polit. Sociol.* **8**, 121–144 (2014).
32. Zuboff, S. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *J. Inf. Technol.* **30**, 75–89 (2015).
33. Health, B. M.-T. L. D. & 2020, undefined. Shut down and reboot—preparing to minimise infection in a post-COVID-19 era. *thelancet.com*
34. Hekmati, A., Ramachandran, G., Krishnamachari, B. & Krishnamachari, B. 2020. CONTAIN: Privacy-oriented Contact Tracing Protocols for Epidemics. *arxiv.org* (2020). doi:10.1145/nnnnnnn.nnnnnnn
35. Berke, A., Bakker, M., Vepakomma, P., Larson, K. & Sandy' Pentland, A. '. *Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy*. *arxiv.org* (2020).
36. Bell, J., Butler, D., Hicks, C. & Crowcroft, J. TraceSecure: Towards Privacy Preserving Contact Tracing. (2020).
37. ISO. Health informatics — pseudonymization. (2017).
38. Ding, X., Zhang, L., Wan, Z. & Gu, M. A brief survey on de-anonymization attacks in online social networks. in *Proceedings - International Conference on Computational Aspects of Social Networks, CASoN'10* 611–615 (2010). doi:10.1109/CASoN.2010.139
39. Lai, L. Coronavirus: Singapore to review strategy if cases climb. *The Straits Times* (2020).
40. Aravindan, A. & Phartiyal, S. Bluetooth phone apps for tracking COVID-19 show modest early results. *Reuters* (2020). Available at: https://uk.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUKKCN2232A0. (Accessed: 8th May 2020)
41. NDI{API}. SafeEntry. *NDI{API}* (2020). Available at: https://www.ndi-api.gov.sg/safeentry. (Accessed: 8th May 2020)
42. Singaporean Government. Digital contact tracing tools for all businesses operating during circuit breaker. *Singaporean Government* (2020). Available at: https://www.gov.sg/article/digital-contact-tracing-tools-for-all-businesses-operating-during-circuit-breaker. (Accessed: 8th May 2020)
43. Mozur, P., Zhong, R. & Krolik, A. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags - The New York Times. *New York Times* (2020).
44. Creemers, R. China's Social Credit System: An Evolving Practice of Control. *SSRN Electron. J.* (2018). doi:10.2139/ssrn.3175792
45. Digital health. NHSX differs with Apple and Google over contact-tracing app. *Digital health* (2020).
46. Memon, N. How Biometric Authentication Poses New Challenges to Our Security and Privacy

[In the Spotlight]. *IEEE Signal Process. Mag.* **34**, 194–196 (2017).
47. Newman, N. The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google. *SSRN Electron. J.* (2013). doi:10.2139/ssrn.2310146
48. Digital health. Covid-19: NHS contact-tracing app launched in Isle of Wight. *Digital health* (2020). Available at: https://www.digitalhealth.net/2020/05/covid-19-nhs-contact-tracing-app-launched-in-isle-of-wight/. (Accessed: 8th May 2020)
49. medConfidential. GCHQ and NHSX's contact tracing app. *medConfidential* (2020). Available at: https://medconfidential.org/2020/gchq-and-nhsxs-contact-tracing-app/. (Accessed: 8th May 2020)
50. Big Brother Watch. FAQ: Everything you need to know about the NHSX contact tracing app. *Big Brother Watch* (2020). Available at: https://bigbrotherwatch.org.uk/campaigns/emergency-powers/faq/. (Accessed: 8th May 2020)
51. The New York Times. Spy Contractor's Idea Helped Cambridge Analytica Harvest Facebook Data. *The New York Times* (2020). Available at: https://www.nytimes.com/2018/03/27/us/cambridge-analytica-palantir.html. (Accessed: 8th May 2020)
52. Evans, R. & Pegg, D. Vote Leave AI firm wins seven government contracts in 18 months. *The Guardian* (2020).
53. Cellan-Jones, R. Coronavirus: Hands on with NHS Covid-19 contact-tracing app. *BBC News* (2020). Available at: https://www.bbc.co.uk/news/technology-52551273. (Accessed: 8th May 2020)
54. Busvine, D. & Rinke, A. Germany flips to Apple-Google approach on smartphone contact tracing - Reuters. *Reuters* (2020). Available at: https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J. (Accessed: 8th May 2020)
55. Kelion, L. Coronavirus: NHS reveals source code behind contact-tracing app. *BBC News* (2020). Available at: https://www.bbc.co.uk/news/technology-52579547. (Accessed: 8th May 2020)
56. NHSX. Source code of the Beta of the NHS COVID-19 iOS app. *GitHub* (2020). Available at: https://github.com/nhsx/COVID-19-app-iOS-BETA. (Accessed: 8th May 2020)
57. Hern, A. & Proctor, K. UK may ditch NHS contact-tracing app for Apple and Google model. *The Guardian* (2020).
58. Ryder, J. *Data Protection Impact Assessment NHS COVID-19 App PILOT LIVE RELEASE Isle of Wight 2 Data Protection Impact Assessment ('DPIA')*. (2020).
59. UK Government. NHS COVID-19: the new contact-tracing app from the NHS. *UK Government* (2020). Available at: https://www.ncsc.gov.uk/information/nhs-covid-19-app-explainer. (Accessed: 8th May 2020)
60. Information Commissioner's Office. Statement in response to media enquiries about the Data Protection Impact Assessment for the NHSX's trial of contact tracing app. *Information Commissioner's Office* (2020).
61. House of Commons. Science and Technology Committee Oral evidence: UK Science, Research and Technology Capability and Influence in. *House of Commons Library* (2020). Available at: https://committees.parliament.uk/oralevidence/316/html/. (Accessed: 8th May 2020)