Pump
Court

Contact Tracing – The Ethical and Legal Issues

Anthony Speaight KC, Iain Munro and Anna Hoffmann

Three members of chambers examine the ethical debate and legal issues surrounding the adoption of a contact tracing app. They conclude that the technology which the British Government has to date favoured raises a host of ethical dilemmas and legal challenges.

The technological responses to the pandemic have been profound, controversial and are evolving quickly, with some predicting lasting cultural changes.

Tools for virtual communication and collaboration have a forced prevalence. While virtual court hearings, arbitrations and mediations have long been possible, uptake has sharply increased – a form of hearings on which opinions vary. Some practitioners consider that if the practices of the lockdown period are maintained after it ends, access to justice would be improved for those with the necessary skills and equipment. Others consider that virtual trials diminish the effectiveness of cross-examination, reduce the impact of advocacy and promote over-simplification.

Within the health sector, the innovations have been far reaching as well. For example, within hospitals, in-room professionals have used mixed reality headsets when they treated COVID patients, limiting exposure of a wider specialist team, who can join from a safe space and yet see, hear and communicate.[1] Not everything is so cutting edge: for example, conventional messaging systems have helped reduce the spread and wireless headsets have improved communication wearing PPE. In the primary care context, use of digital triage and telemedicine (e.g., eConsult, Cinapsis, Babylon) has spiked. Virtual GP visits are being coupled with contact-free assessment tools, so that physical attendance at care homes is reduced.[2] Some of these apps allow for immediate input from consultants, avoiding further referrals. COVID testing (via saliva, fingerprints etc) has been another vital area of innovation.

Some of the most controversial innovations relate to smartphones and other monitoring devices, as they offer the potential capability for unprecedented surveillance of people's movements, contacts, and health. Examples of such technologies are increasing rapidly:

- Anonymised location tracking data has been provided by Apple and Google to help assess the efficacy of lockdowns.
- Wearable tech, like FitBits, is hyped as a way of monitoring the spread of the virus, through use of temperature and other data.[3]
- Device owners can also use apps aimed at detecting or diagnosing COVID before display of symptoms.[4]
- The "COVID Symptom Study" app has allowed comparison of symptoms with confirmed cases, contributing to our understanding of the virus.[5]
- Contact tracing apps are being developed by over 30 countries[6] as a means of identifying and containing new cases. Smaller scale, commercial products are also available (e.g. "CarePredict"
- for care homes[7]). These apps can be combined with accessories, such as electronic bracelets, for closer monitoring.
- In China, a variety of measures have been combined with a system of QR codes which must be scanned at entrances to public transport, shops and other spaces. Those who are required to isolate are denied entry. It has been suggested that the city of Hangzhou might permanently assign health badges, based on medical records and lifestyle.[8]

- As a more limited formulation, Singapore operates a digital check-in system (“SafeEntry”) which logs the identity card and mobile phone numbers of visitors to a variety of locations.[9]
- More frivolous uses of smartphones include “Remote Cheerer”, which may bring the sounds of fans to empty sporting venues.[10]

Of these new technologies none is currently the subject of as much argument in the UK as the topic of this paper – contact tracing.

How contact tracing technologies work

The value of tracing the contacts of individuals infected with COVID, so far as it can be achieved, is universally recognised. There is also wide acceptance that, faced with the gravity of the current emergency, it is worthwhile to attempt to trace infectious contacts through a smartphone app, although there is as yet no certainty as to how much this will achieve.

A significant debate which has emerged is between the two main models: they are often referred to as, respectively, the centralised, and the decentralised model.

The two models start at the same place. Users install software on their smartphones, which exchanges anonymised – or some might say pseudonymous – signals (“identifiers”, “codes” or “keys” of randomly generated numbers) with nearby users via Bluetooth technology. For simplified description of how it works,[11] let us imagine two individuals, A and B, both of whom have installed the app on their smartphones. A and B meet each other in a park and sit talking on a bench. Both phones share and store each other’s signals. Later A tests positive for COVID. A may then choose to notify a central server. There is no compulsion on A to do so, although clearly it is a public-spirited action and one which the user probably had in mind when deciding to install the app.

Under the centralised model, users send the codes they have collected, along with their own identifier, to a usually national database. The central server then records the contacts, performs analysis and sends out alerts to smartphones, such as that of B.

Under the decentralised model, A’s smartphone sends to a central point only A’s own identifier if and when A chooses to report the onset of infection. The central server regularly sends out to all app users the list of the infected. The app on B’s phone looks for matches between the identifiers on the infected list and identifiers which the phone has stored over a recent period. If B’s app spots a match, then B’s own phone generates an alert to B.

The key distinction therefore is where and how the data is stored. From this flows access to knowledge and the ability to delete personal data. Under the decentralised, but not under the centralised, the fact of A and B having been in contact is not communicated to the central authority by operation of the app;   under the one, but not under the other, the fact that B has been notified of the contact is intended to be private to B; under the one, but not under the other, B receives no governmental communication telling B to do anything. Under the centralised model, B has no ability to delete from the operators’ databank the record of the contact: under the decentralised app, the question of such deletion does not arise because the operator has never had B’s personal data in the first place.

Britain has an available option of both models. A central unit concerned with health technologies, called NHSX,[12] has developed a version of a centralised app. The NHSX app has been piloted in the Isle of Wight, where the government has claimed the pilot was a success. A decentralised app has been developed from work called DP3T by an international group of academics including Dr Michael Veale of UCL. This model has been taken up Apple and Google, who by joint working have made available an app which they call the Contact Tracing Framework. The Information Commissioner has published a favourable opinion on the Apple/Google app.[13]

In addition to the features discussed above, there are other important differences between the emergent apps. For example:

1. Some apps use GPS technology to record actual locations and report this information to the central server. The South Korean tracing app uses GPS data not only to trace contact but also to check whether quarantine orders are observed. Israeli and Pilipino apps ("HaMagen" and "WeTrace" respectively) also use location data. So far, the European apps under development appear to only track proximity, rather than actual, specific location.

2. When it comes to reporting an infection, almost every other Western country will require a COVID diagnosis confirmed by a positive test.[14] The NHSX scheme invites users to report self-diagnosis of symptoms, and is designed to send out alerts to contacts as soon as such is received. Since self-diagnosis is uncertain, and there is much experience of individuals being unsure whether they have symptoms or not, this system will result in false alerts, subjecting contacts to potential worry, inconvenience and "notification fatigue".[15] However, Professor Christopher Fraser of the University of Oxford's Big Data Institute has defended this approach, explaining that it is justified by epidemiological models for a virus which is transmitted quickly, before people acquire symptoms.[16] Reliance on positive results also demands ready availability of testing. Proponents of the centralised model say it enables the app to 'unwind' notifications more easily.[17]

3. Technological variety gives rise to issues of interoperability. Systems based on a common standard (such as the Apple/Google API) will find it easier to surmount them. Interoperability between the NHSX app and decentralised counterparts is a recognised challenge.[18]

More generally, the efficacy of all approaches depends on user uptake and needs to be complemented by an effective manual tracing system. Singapore's decentralised app, "TraceTogether",[19] had been downloaded by around 25 percent of residents, far short of the 75% percentage thought to be needed. However, as employers are required to introduce a tracking system for returning workers (such as "TraceTogether"), the position may change.[20] Uptake is reportedly much higher in China, where usage of a tracing app appears to have become a practical necessity [21].

The Ethical Debate

The ethical debates about contact tracing are international. The legal framework is pan-European. A mature assessment of the choice facing Britain calls for a much wider focus than a purely national one. Of particular relevance to Britain are the current fast-moving debates in France and Germany – which are, like the UK, subject to the GDPR and in Switzerland[22].

Most European countries are adopting a decentralised approach. Germany, which had originally proposed a centralised app, has ended up switching to a decentralised system. France, on the other hand, has made a firm decision for a centralised system. In the UK, as mentioned, the Government has piloted the NHSX centralised system; but it may change direction and there are some indications of hesitation, at least. NHSX has awarded a £3.8M contract to the London office of Zuhlke Engineering, a Switzerland-based IT development firm which was involved in developing the initial version of the NHSX app. The contract reportedly includes a requirement to "*investigate the complexity, performance and feasibility of implementing native Apple and Google contact tracing APIs within the existing proximity mobile application and platform*".[23]

The United Kingdom

The concern which has most strongly been expressed in Britain is of "mission creep". Although the initial version of the NHSX scheme involves the central pool of information containing little more than the fact of the contact between A and B, there are indications that NHSX is interested in expanding the amount of information which it will obtain. Indeed, the very reason for its preference for a centralised system over a decentralised system is this very possibility of increasing the information obtained. Giving evidence to the Parliamentary Joint Committee on Human Rights on 4th May 2020, CEO of NHSX, Mr Matthew Gould,[24] said:-

> "[I]f privacy were the only thing that we were optimising for, a decentralised approach could well be the default choice. But, actually, we are balancing a number of things. We are balancing privacy with the need for the public health authorities to get insight into what symptoms subsequently lead to people testing positive, for example, which kinds of contact are riskier, and what changes occur in the nature of contact between, say, three days and one day before symptoms develop."

So, the first point to notice is that the explicit justification for the choice of the centralised system is its capacity to acquire more information. That is not in itself a criticism: the acquisition of information about how the virus spreads is plainly in itself a public good, and one which NHS epidemiologists are properly keen to maximise. The issue is the potential for the system, once in place, to be extended.

That some expansion of the information collected is envisaged by NHSX is frankly admitted. In a blog post[25] Mr Gould has written with Dr Geraint Lewis, it is suggested:

> "In future releases of the app, people will be able to choose to provide the NHS with extra information about themselves to help us identify hotspots and trends."

Mr Gould told the Parliamentary Committee:-

> "If you have a centralised approach, it becomes more straightforward to hone your understanding and decision-making inside the app, which will allow you, for example, to make sure that symptoms become more accurate over time and you get a better understanding of when the most dangerous time in somebody's development of symptoms is for them to be having proximity events. Over time, it will tell us whether, for example, five minutes at one metre away is rather more important than 15 minutes at two metres away."

So NHSX hope to collect information not just on the date of A's meeting with B, but also on how long they were in contact and how closely they sat on the park bench. This kind of information is a common target of contact tracing apps, as it informs the likelihood of infection.[26]

Again, the possession of such information by researchers may not in itself be a bad thing. The point at this stage is simply to observe that NHSX hope in future to expand the information which they collect through the app. The concern is how far the mission creep might go.

At present NHSX heavily stress that the installation of the app and its use are voluntary. But suspicions lurk that some elements in authority may envisage linking the removal of some lockdown restrictions with use of the app. Mr Alex Wickham, the Political Editor of Buzzfeed, claiming sources for his piece, wrote on 18th April 2020[27]:-

> "The concerns of some commentators about how the NHSX app could be used have not been assisted by

> the requirement, despite the protestations that locality is not being traced, for users to supply the first part of their postcode. The justification offered is the NHS desire to track where there may be demand for hospital facilities. Yet the NHS already has an abundance of information on this, as manifested by the publication of data on the incidence of infection by districts. So some people have sensed a natural inclination of public sector administrators to hoover up as much data as they can."

Another concern heard in Britain is of social exclusion if any disadvantages were to be introduced for individuals who do not carry a smartphone with the app installed. Some citizens cannot afford to acquire a smartphone, and some people, especially the elderly, have difficulty in knowing how to download or use an app. Smartphone adoption reached 78 percent during the first half of 2018. However, smartphone ownership drops off steeply for users aged 55 or older, with just 55 percent of residents in that age group reporting that they own a smartphone.[28]While smartphone ownership will likely have increased since then, it does highlight that the elderly would face particular challenges with the app.

The possibility of detriments for non-use is not confined to the theoretical, if improbable, scenario of government-imposed sanctions. It could happen in the private sector: an employer might require its workers to use the app, or a shop might admit only customers who carry a phone with an app installed. Such detriments would tend to affect the most vulnerable groups.

These fears could be dispelled if the Government were to accept a well-developed proposal for legislation embodying safeguards. Professor Lilian Edwards of Newcastle University, leading a team of academics from eight universities, has published a draft Coronavirus (Safeguards) Bill.[29] This Bill would prohibit sanctions of any kind for failing to carry a phone on which the app had been installed. The promoters of this Bill argue that this would enhance public trust and thus increase uptake. It would also protect the digitally excluded portion of the population from discrimination. To date there has been no sign of willingness on the part of the Department of Health to accept such legislation. There has been no White Paper, and no parliamentary debate. In the absence of the enactment of such safeguards to install the app the question inevitably remains, "If you do not intend detriments on non-users of the app, why will you not accept this Bill?"

In the light of these issues discussed in this article, the all-party Parliamentary Joint Committee on Human Rights has unanimously advised that the Government should not rollout the NHSX app until important steps have been taken[30]. The Committee has published its own draft Bill. This does not go as far as Professor Edwards' Bill, but it would establish a Digital Contact Tracing Commissioner whose remit would be wider than that of the Information Commissioner, bringing in a responsibility for discrimination, and all political freedoms, as well as just data protection. The Committee calls for the highest standards of data security, and for the deletion of all data at the latest after 2 years. Concerns have been raised over the narrow ambit a new "Digital Contact Tracing Commissioner" would have, which may render this office unable to deal with other technological responses to the pandemic that go beyond contact tracing.[31]

Even if the NHSX app remains the Government's preference, it should, perhaps, be noted that health is a devolved competence. It cannot be certain that the devolved administrations will favour it. The teams which NHSX unit brings together are from NHS England and a central government department whose work today is almost entirely confined to responsibilities in England.

The government has published a Data Protection Impact Assessment (a "DPIA")[32] about this pilot project on the Isle of Wight, concluding that:-

> "The Department of Health and Social Care, has determined that any interference with the private life of users caused by the operation of the App is (i) in accordance with the law (in that the public authority (DHSC) has a legal basis to carry out the relevant personal data processing, and has the vires necessary to

> operate a public health App); and (ii) is a necessary and proportionate measure in a democratic society, in pursuit of the legitimate aim of ensuring public safety. Our demonstrable compliance with data protection legislation and the common law duty of confidence underpin this." (p.5)

However, this DPIA has come in for severe criticism. Dr Michael Veale of UCL states for example[33] that it is wrong to claim that the data will be anonymous and that the right to access and erasure have not been adequately dealt with.

Germany

The German plans for a contract tracing app are particularly interesting for the centralised vs decentralised app debate, as the German government changed its plan mid-course, switching from a centralised to a decentralised model, after the centralised model came in for severe criticism, *inter alia* in the form of an open letter signed by hundreds of leading scientists, including many UK signatories. In this joint statement, the scientists warned of the dangers of a location tracing application, i.e. an application that would trace the physical location of a phone via GPS and/or network information as well as centralised proximity tracing apps:-

> "Research has demonstrated that solutions based on sharing geolocation (i.e., GPS) to discover contacts lack sufficient accuracy and also carry privacy risks because the GPS data is sent to a centralized location. For this reason, Bluetooth-based solutions for automated contact tracing are strongly preferred when available. Some of the Bluetooth-based proposals respect the individual's right to privacy, whilst others would enable (via mission creep) a form of government or private sector surveillance that would catastrophically hamper trust in and acceptance of such an application by society at large. It is crucial that citizens trust the applications in order to produce sufficient uptake to make a difference in tackling the crisis. It is vital that, in coming out of the current crisis, we do not create a tool that enables large scale data collection on the population, either now or at a later time. Thus, solutions which allow reconstructing invasive information about the population should be rejected without further discussion"[34]

The German "Corona Warn" app is currently being developed in cooperation between the Fraunhofer Institut für Nachrichtentechnik (Heinrich-Hertz-Institut), the Robert-Koch-Institut and the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Security in Information Technology). The Bundesdatenschutzbeauftragte (The Data Protection Commissioner) is also consulting the project and the German army is assisting in simulating everyday interactions in order to test the app.[35] The focus of the app is on measuring the distance between users and length of contact and omitting location tracing completely. It is open source, decentralised and relies on Bluetooth and the Exposure Notification Framework provided by Apple and Google. The official website is already online and emphasises transparency and data protection[36]; however the app has not yet been launched nationwide.

Even though Germany has opted for a decentralised app, a fierce debate has started amongst data protection watchdogs and also constitutional lawyers as to the validity of consent to an app, the comparability of the present situation pandemic with factual scenarios forming the basis of existing data retention case law and whether it is really a better idea to build and rely on non-state actors / corporations such as Apple and Google rather than the state.[37]

Switzerland

Switzerland has already launched a version of its tracing app, the "SwissCovid" app and is the first to use the updated Apple/Google API (application programming interface). The decentralised contact tracing app, developed by the two Swiss federal institutes of technology in Zurich (ETH Zurich) and Lausanne (EPFL) has been in testing since 13th May 2020 but will only be rolled out to the wider population after parliament has created a new legal basis for the app. In its official "questions and answers" publication, the Swiss government describes the app's functionality in these terms:-

> "The SwissCovid app only records contacts, i.e. when its user is less than two metres distance from another SwissCovid app user for a short period of time. Details of these contacts are stored decentrally, i.e. on the user's own mobile phone, in the form of a cryptographically generated checksum; after 21 days, these data are irretrievably deleted. This means that there is no exchange of personal data, locations or information about the device used. In the event of a contact, all that is exchanged is an encrypted code. This is saved locally on the devices concerned and then automatically deleted 21 days later. This applies both to the data in the local memory of the mobile phone and to the keys related to infected users on the Federal Administration server. If the SwissCovid app is uninstalled, the data on the mobile phone is automatically deleted."[38]

There has been a motion in both Swiss Parliamentary Chambers which demanded that new legislation be passed in relation to this app, enshrining that no personal data would be retained centrally and that use of the app would remain voluntary.[39] Crucially the motion also demanded that no access to services could be limited by demanding use of an app. The Bundesrat (the executive) first rejected this motion, arguing that the "Epedemiegesetz" (the pandemic law) was sufficient as a legal basis for the app. However, the majority of the Swiss Parliament adopted the motion and the government will have to formulate a full Federal Law which is to be discussed and passed by Parliament in early June 2020. The earliest the "SwissCovid" app could thus be available to the wider public is July 2020.[40] The Swiss experience is a clear example of a legislative/deliberative body demanding that some time be spent on formulating an appropriate legal basis for new technologies, including safeguards, even in a time of acute crisis, in order to address data protection concerns and safeguards against detriments arising from non-use.

France

Similarly, the French required a parliamentary debate and vote before rolling out their centralised "StopCovid" app. The app is set to be released in the first week of June to supplement the manual contact tracing that is already taking place. On 24th April 2020, the French data protection authority ("CNIL") published its opinion about the app[41]. It made clear its view that a centralised app, such as "StopCovid" as well as the NHSX app, would be subject to the GDPR requirements:-

> "Firstly, it should be pointed out that in order to be able to inform a user of a possible exposure to the virus, the central server must check whether there is a match between the pseudonyms attributed, at the time of its installation, to that user's application and those transmitted to the central server by the application of another person which has been diagnosed as positive. The result is that there remains a link between the pseudonyms and the downloaded applications, each application being itself installed on a terminal, which generally corresponds to a specific natural person. As a result of this link, the Commission considers that the device will process personal data within the meaning of the GDPR. Furthermore, the collection of temporary pseudonyms of the persons with whom the user has been in contact could allow the reconstruction of all the relationships the user has had with other users of the application. In the light of these factors, the Commission considers that the planned system is subject to the rules on the protection of personal data, while recognising that the safeguards taken provide a high degree of guarantee to minimise the risk of re-identification of the natural persons associated with the data stored, for a necessarily limited period, by the central server."

CNIL suggested a number of technical safeguards including high-level organisational and technical security measures, state-of-the-art cryptographic algorithms and unrestricted access to the source code.

There have been many concerns raised about the centralised "StopCovid" app, most also citing the potential for mission creep as well as potential for abuse as key weaknesses. Hundreds of French academics have signed an open letter calling for more safeguards.[42] One of the recommendations in the CNIL opinion was to make sure that geolocating, i.e. location tracing, would not be possible. This goes back to the differentiation made above. It should not be possible for any authority to know where A and B met, but only that they were in a defined proximity range to each other and potentially also how long this meeting lasted. However, it has been claimed by programmers working on the app that the ROBERT protocol it uses does require fine grained location permission via GPS.[43]

If that claim is accurate the ROBERT protocol would not comply with the recommendation of the European Data Protection Board (EDPB), which in its recent guideline on tracing apps[44] stated that:-

> "In this regard, the EDPB has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users."[45]

Part of the reasoning behind the centralised approach was set out by the Secretary of State for the Digital Sector of France, Cédric O,[46] who pointed out that opting to not use the Apple/Google protocol was also a question of sovereignty:-

> "Health policy is, from the point of view of the French government, a sovereign prerogative which is the responsibility of the state. It is up to the public authorities, with their qualities and their faults, to make the choices they consider to be the best for protecting French women and men. The French government does not refuse the API proposed in the state by these two companies because they are American companies. (…) It refuses to do so because, in its current format, it constrains the technical choice: Only a 'decentralized' solution can work perfectly on phones equipped with iOS (…) [France] must not to be constrained by the choices of a big company, as innovative and efficient as it is."

The Legal Issues

The GDPR

The EU General Data Protection Regulation currently remains in force in the UK. Since 31st January 2020, when the UK exited the EU, the GDPR is effective by virtue of the EU (Withdrawal Agreement) Act 2020.[47] After the end of the implementation period, which by law is currently 31st December 2020, provisions, which in substance are identical, will be operative under what is to be known as UK GDPR. That will be achieved by the EU's GDPR remaining in force in the UK by virtue of the carry over provisions in the EU (Withdrawal) Act, subject to modifications made by a statutory instrument.[48] UK GDPR provisions will have no substantive difference to the provisions of the EU GDPR discussed in the following paragraphs.

Is processing of personal data involved?

The starting point in an analysis of the law affecting a tracing app is to determine whether the model involves processing personal data.

Despite some protestations from the NHSX to the contrary, in our opinion a court will be likely to consider that the NHSX scheme involves the processing of "personal data". "Personal data" means information relating to an identified or identifiable living individual[49]. Most commonly identification is by the individual's name, but it can be in other ways. This includes data which, in the data protection jargon, "individuates" a person. In *Vidal-Hall v Google* in 2016 the Court of Appeal was concerned with the information about websites visited by a computer browser, which is known as browser generated information or BGI. The judgment of Lord Dyson, Master of the Rolls, stated[50]:-

> "Identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others. It is immaterial that the BGI does not name the user."

Since the very function of the central server in the NHSX's app is to differentiate A from every other user of the app, it individuates A. That remains so, despite A's identity being pseudonymous. Furthermore, the system enables NHSX to build up a picture of everybody with whom A has been in contact, from which identification could occur.

For similar reasons, the French app would also seem to involve processing personal data. We have already observed that that is the opinion of the French data protection authority. The EDPB has issued another guideline recently[51], in which it states that while the GDPR "*foresees a specific derogation to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for these purposes of scientific research*" but that nevertheless "*Fundamental Rights of the EU must be applied when processing health data for the purpose of scientific research connected to the COVID-19 pandemic*."

By contrast, we see no likely basis for a court to hold that the Apple/Google scheme involves the processing of personal data. The Information Commissioner, who has published no concluded opinion in respect of NHSX, has issued an opinion that Apple/Google scheme does not involve the processing of personal data.[52] Accordingly, we see no particular legal problems in the way of the roll out of a decentralised system in the UK, if the Government were to change its position and promote such.

In respect of the NHSX app, granted that processing of personal data is involved, the next question is whether there is a route to avoid the default position of the prohibition on the processing of personal data outside defined situations.[53] In simple terms, there are two main gateways to permissible processing: one is consent, the other necessity for a public interest. Neither gateway will be straightforward for NHSX.

The difficulty in passing the consent gateway

In practise, the consent of the data subject is by far the most common basis for processing personal data – as we are all made so aware by the frequency with which we are irritated by computer requests to consent to this or that. NHSX may argue that consent exists since installing the app is voluntary, and since uploading a notification of infection is also voluntary. But there are several problems with that argument. To be valid, consent must be a "*freely given, specific, informed and unambiguous indication of the data subject's wishes*"[54]. It is hard to demonstrate the giving of consent to a public authority owing to the imbalance of power between such an authority and an ordinary citizen[55].This would be even more so if the use of the app was a practical necessity for accessing work or services.

Next consent must be given not just at large but for the specific purpose in question: a data subject may consent to a controller processing for one purpose but not to processing for a distinct purpose.[56] Thus consent given to processing by the NHSX central server for the purpose of contact tracing may not extend to the purpose of the NHSX building up a broader profile of the population for research purposes.

Finally, it is a facet of valid consent that it may be withdrawn at any time, and that "*it shall be as easy to withdraw as to give consent*"[57]. Mr Gould admitted to the Joint Parliamentary Committee that once a user had uploaded information on his or her infection, it would not be possible to accede to a request from the user to cease processing of that data:-

> "Q: Once someone's data has been sent to the centralised collection area, can that person request that their data is deleted?
>
> M. Gould: No. The data can be deleted as long it is on your own device. Once it is uploaded, it becomes enmeshed in wider data, and the technical difficulties of deleting it at that point become tricky."

The difficulty in passing the public interest gateway

If, then, passing through the consent gateway is uncertain, what about a public interest argument? Data relating to health faces a stiffer test than less sensitive information about an individual. The most promising routes would appear to be those set out in GDPR Article 9 as for the public interest in the area of public health, or other substantial public interest:-

> GDPR Article 9(2)(I): "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;"
>
> GDPR Article 9(2)(g): "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"

Plainly the present situation would fit into such public interest categories. The requirements then are:

(a) a necessity test – that the public interest makes the processing of personal data necessary;

(b) safeguards in law – member state law providing suitable and specific measures to safeguard rights and freedoms.

As to the necessity test, the threshold is high: "necessary" is a strong word. In the UK Supreme Court, Lord Kerr recently characterised this as meaning "*strictly necessary*".[58] It involves a proportionality analysis.[59] Lord Sumption, in the Supreme Court, has said that a proportionality assessment involves considering whether a less intrusive measure could have been adopted without unacceptably comprising the objective[60]. Granted the availability of the decentralised

Apple/Google scheme, the challenge then for NHSX is to demonstrate further public interest objectives which only a centralised scheme can achieve.

If that is achieved, the NHSX app will face, as matters stand at present, a further challenge with the requirement for a UK law providing specific measures to safeguard the rights and freedoms of data subjects. Such would be likely to be achieved if Parliament were to enact legislation along the lines of Professor Edwards' draft Bill. Almost every commentator, as well as the Parliamentary Human Rights Committee has urged the Government to enact specific safeguards, or to establish an oversight authority, or both. To date, however, there has been no intimation of any Government intention to present any legislation at all relating to a tracing app.

Transparency

A further challenge for the NHSX app is to satisfy the first data protection principle, which is that the processing of personal data must be not only lawful and fair, but also transparent. Partly to satisfy transparency the GDPR requires that Data Protection Impact Assessment ("DPIA") where processing is likely to result in a high risk to the rights and freedoms of individuals. The European Data Protection Board has also expressed the opinion that there should be a DPIA before implementing apps.[61] NHSX published such an Impact Assessment on the eve of the going live of its app in the Isle of Wight. Unfortunately, this Assessment has not met with approval from specialists in the field. In a searing critique,[62] mentioned above, Dr Veale of UCL has described it as "*legally misleading*", internally contradictory, "*confusing*" and involving the denial of the right of erasure without a specified legal reason for doing so.

Fundamental Rights

Some commentators have suggested a major role in determining the legality of a centralised app for Article 8 of the EU Charter of Fundamental Rights, which provides:-

> "1. Everyone has the right to the protection of personal data concerning him or her
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified…."

If the NHSX app can clear the data protection law hurdles which we have already set out, we do not consider that the EU Charter would pose any additional hurdle for it to clear. The protections required by the Charter are already achieved in a detailed and specific way by the GDPR. Furthermore, the Charter as such ceased to be a part of domestic law on 31st January 2020[63]. However, there remain in domestic law until the implementation day[64] both the general principles of EU law, of which one is the right to an effective remedy, and the fundamental rights of EU law, which include those of data protection.

Lawyers may recall that the potency of fundamental rights law in this field was dramatically demonstrated by *Vidal-Hall v Google*[65]. A group of computer users complained about Google accessing details of their internet usage. They had suffered no financial loss but claimed general damages for distress and anxiety. The Data Protection Act 1998, which was then the governing statute in Britain, by s.13(2) specifically excluded the recovery of general damages by a claimant who had suffered no financial loss. The Court of Appeal was persuaded that the EU Directive, which was given effect by the 1998 Act, had intended to require the possibility of general damages in all cases; and that accordingly the Act had failed effectively to transpose the EU Directive into domestic law. The Court was emboldened to "disapply", or in layman's language to strike down, s.13(2) of the UK statute by reason of the EU Charter of Fundamental Rights.

Fundamental rights considerations do not solely depend on EU-derived law. The European Court of Human Rights has on several occasions[66] held that the collection by the state of data about an individual engages the right to respect for private life in Article 8 of the European Convention on Human Rights.

Therefore, whilst we do not see fundamental rights charters are creating an additional hurdle for a tracing app to clear, we do consider that they set an atmosphere in which the primary question of compliance with data protection law can be expected to be addressed by a court with anxious scrutiny.

Conclusion

The version of a contact tracing app, the NHSX app, which the Government has piloted, and claimed to be a success, raises a host of issues. Many commentators have expressed ethical concerns, mirroring those which featured in the debates in other European countries, both within and outside the EU. The all-party Parliamentary Joint Committee on Human Rights has called on the Government not to roll out the NHSX app until legislation has been enacted establishing an oversight Commissioner. Considerable interest has been generated by a draft Bill prepared by a group led by Professor Lilian Edwards, which would go further and prohibit any detriments being placed on those, who by reason of digital exclusion or personal privacy preference, do not carry a smartphone on which the app is installed. The NHSX faces challenges to show that it complies with data protection law: this will remain as true after the end of the Brexit implementation period as it is now.

Please note that this paper does not provide legal advice. Whilst every care has been taken in the preparation of this document, we cannot accept any liability for any loss or damage, whether caused by negligence or otherwise, to any person using this document.

[1] https://www.bbc.co.uk/news/av/health-52692298/coronavirus-mixed-reality-headsets-help-medics-treat-covid-19-patients (accessed 1st June 2020).

[2] https://www.mobihealthnews.com/news/europe/wi-fi-nightingale-virtual-gp-carehomes-and-new-technologies-related-covid-19 (accessed 1st June 2020).

[3] See, e.g., https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30222-5/fulltext (accessed 1st June) regarding the use of resting heart rate and sleep measures for evaluating population trends of seasonal respiratory infections, such as influenza.

[4] https://www.mobihealthnews.com/news/fitbit-launches-covid-19-wearables-study-early-detection-algorithm (accessed 1st June 2020).

[5] https://covid.joinzoe.com/ (accessed 1st June 2020).

[6] https://www.wired.co.uk/article/nhs-covid-19-tracking-app-contact-tracing (accessed 1st June 2020).

[7] https://www.carepredict.com/press-releases/carepredict-announces-pinpoint-toolset-breakthrough-contact-tracing-technology-for-senior-living-facilities/ (accessed 1st June 2020).

[8] https://www.reuters.com/article/us-health-coronavirus-china-tech/as-chinese-authorities-expand-use-of-health-tracking-apps-privacy-concerns-grow-idUSKBN23212V (accessed 1st June 2020).

[9] https://www.safeentry.gov.sg/ (accessed 1st June 2020).

[10] https://www.theguardian.com/world/2020/may/27/japan-launches-remote-cheering-app-to-boost-atmosphere-in-empty-stadiums (accessed 1st June 2020).

[11] See the flow chart at https://www.bbc.co.uk/news/technology-52355028 (accessed 1st June 2020) and also the

summary at https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app (accessed 2nd June 2020).
[12] A technology unit bringing together teams from the Department of Health and Social Care, NHS England and NHS Improvement.
[13] Information Commissioner's Opinion dated 17th April 2020 on 'Apple and Google Joint Initiative on COVID-19 Contact Tracing Technology' https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf (accessed 1st June 2020).
[14] This follows European Commission advice – see 'Mobile Applications to Support |Contact Tracing in the EU's fight Against COVID-19' 15th April 2020 at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf (accessed 1st June 2020).
[15] See, e.g., the criticisms expressed by Ms Polly Sanderson of the think tank Future of Privacy Forum https://www.digitalhealth.net/2020/05/centralised-approach-to-contact-tracing-app-based-on-shaky-assumptions/ (accessed 2nd June 2020).
[16] Oral evidence to the House of Commons Science and Technology Committee on 28th April 2020 https://committees.parliament.uk/oralevidence/316/html/ (accessed 2nd June 2020).
[17] https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app (accessed 2nd June 2020).
[18] Oral evidence of the CEO of NHSX, Mr Matthew Gould, to the Parliamentary Joint Committee on Human Rights at https://committees.parliament.uk/oralevidence/334/html/ (accessed 1st June 2020).
[19] For a description of how it operates, see Findlay et al (2020) 'Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post crisis'; SMU Centre for AI & Data Governance Research Paper No. 2020/02.
[20] https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether (accessed 1st June 2020).
[21] https://www.lexology.com/library/detail.aspx?g=99dca469-455d-4f7a-b025-00bf1d10ff6b (accessed 1st June 2020).
[22] Switzerland is not a EU member state but many GDPR provisions have been implemented in national law and Switzerland strives to implement the same level of data protections as the EU
[23] https://www.contractsfinder.service.gov.uk/Notice/2d8c89c5-69d2-4073-88dd-401458a92134?origin=SearchResults&p=1 (accessed 1st June 2020).
[24] Oral evidence at https://committees.parliament.uk/oralevidence/334/html/ (accessed 1st June 2020).
[25] https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/ (accessed 1st June 2020).
[26] https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app (accessed 2nd June 2020).
[27] https://www.buzzfeed.com/alexwickham/coronavirus-uk-lockdown-three-stage-exit-plan (accessed 1st June 2020).
[28] https://www.statista.com/statistics/271460/smartphone-adoption-in-the-united-kingdom-uk/ (accessed 1st June 2020).
[29] https://osf.io/preprints/lawarxiv/yc6xu/ (accessed 1st June 2020).
[30] https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/343/34302.htm (accessed 1st June 2020).
[31] See, e.g., the remarks made by Professor Edwards on the webinar hosted by the Society for Computers and Law on 1st June 2020 https://www.scl.org/events/617-there-can-only-be-one-app-an-scl-webinar-discussing-the-implications-of-the-uk-tracing-app-monday-1-june-2020-11-am-12-30-pm (accessed on 1st June 2020).
[32] 'Data Protection Impact Assessment NHS COVID-19 App Pilot Live Release Isle of Wight' 6th May 2020, https://faq.covid19.nhs.uk/DPIA%20COVID-19%20App%20PILOT%20LIVE%20RELEASE%20Isle%20of%20Wight%20Version%201.0.pdf (accessed 2nd June 2020).
[33] 'Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment', 9th May 2020 at https://mcusercontent.com/3450ca9a08011894f4d1d5f7b/files/364c836f-4633-4a8d-86e6-44f5a985becb/Analysis_of_NH

SX_DPIA.pdf (accessed 1st June 2020).

[34] https://news.rub.de/wissenschaft/2020-04-20-forderung-aus-der-forschung-offener-brief-zu-privatsphaerefreundlicher-corona-tracking-app (accessed 1st June 2020).

[35] https://netzpolitik.org/2020/diese-handy-technologie-soll-covid-19-ausbremsen/ (accessed 1st June 2020).

[36] https://www.coronawarn.app/de/ (accessed 1st June 2020).

[37] *Viz*. the debates hosted on "Corona Constitutional", the crisis podcast hosted by the leading German Constitutional Law Blog: https://verfassungsblog.de/corona-constitutional-17-grundrechte-datenschutz-und-andere-missverstaendnisse/ (accessed 1st June 2020).

[38] https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/situation-schweiz-und-international.html (accessed 1st June 2020).

[39] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20203144 (accessed 1st June 2020).

[40] https://www.netzwoche.ch/news/2020-05-05/parlament-fordert-gesetzliche-grundlage-fuer-contact-tracing-app-des-bundes (accessed 1st June 2020).

[42] https://techcrunch.com/2020/04/27/hundreds-of-french-academics-sign-letter-asking-for-safeguards-on-contact-tracing/ (accessed 1st June 2020).

[43] https://nadim.computer/posts/2020-05-27-stopcovid.html (accessed 1st June 2020).

[45] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf (accessed 1st June 2020).

[46] Original language https://medium.com/@cedric.o/stopcovid-ou-encore-b5794d99bb12 (accessed 1st June 2020) quoted here in English: https://venturebeat.com/2020/05/18/france-offers-a-case-study-in-the-battle-between-privacy-and-coronavirus-tracking-apps (accessed 2nd June 2020).

[47] The 2020 Act inserted a new s.1A(2) into the EU Withdrawal Act 2018 stating: "*The European Communities Act 1972 as it has effect in domestic law … immediately before exit day, continues to have effect in domestic law …*"

[48] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, SI 2019 No 419.

[49] Definition in Data Protection Act 2018, summarising definition in GDPR Article 4(1).

[50] [2016] QB 1003 at [115].

[51] See, e.g., GDPR Article 9 (2) (j) and Article 89 (2).

[52] Information Commissioner's Opinion dated 17th April 2020 on 'Apple and Google Joint Initiative on COVID-19 Contact Tracing Technology' https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf (accessed 1st June 2020).

[53] GDPR Article 6(1): "*Processing shall be lawful only if and to the extent that at least one of the following applies …*"

[54] GDPR Article 4(11).

[55] GDPR recital (43): "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.*"

[56] GDPR Article 9(2): "*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes*" (emphasis added).

[57] GDPR Article 7(3).

[58] *R (El Gizouli) v Home Secretary* [2020] 2 WLR 857 at [158].

[59] *Guriev v Community Safety Development* [2016] EWHC 643 per Warby J at [45]. [1]
[60] *Bank Mellat v HM Treasury* [2014] AC 700 at [20].
[62] 'Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment', 9th May 2020 at https://mcusercontent.com/3450ca9a08011894f4d1d5f7b/files/364c836f-4633-4a8d-86e6-44f5a985becb/Analysis_of_NHSX_DPIA.pdf (accessed 1st June 2020).
[63] S.5(4) EU Withdrawal Act 2018.
[64] S.5(5) EU Withdrawal Act 2018.
[65] [2016] QB 1003.
[66] S and Marper v UK [2008] ECHR 1581. The case concerned the retention of biometric data of persons who had been suspected of an offence but not convicted.