SCL SOCIETY OF CONSERVATIVE LAWYERS

# CONTACT TRACING

## WHAT GOVERNMENT MUST DO TO ACHIEVE TAKE-UP AND SECURE PRIVACY

Guy Sandhurst QC
Benet Brandreth QC
Simon PG Murray

## About the authors

Lord Sandhurst QC is a past Chairman of the Bar of England and Wales (as Guy Mansfield QC), and a current member of the Executive of the Society of Conservative Lawyers.

Lord Sandhurst is leading research on the range of Coronavirus laws, and will be pleased to hear from any member of the Society who is interested in assisting. Please contact via administrator@conservativelawyers.com

Benet Brandreth QC is a former member of the Attorney-General's 'A' Panel of Counsel and a specialist in intellectual property law.

Simon PG Murray is a barrister at 39 Essex Chambers who specialises in public law and human rights. He is on the Attorney General's A Panel.

Each writes in a purely personal capacity. The views expressed in this paper are only those of the authors, and do not represent a corporate opinion of the Society

London, 6 May 2020

---

## INTRODUCTION

On 30th April 2020, the Government announced that it had met its target of 100,000 coronavirus tests a day. Provided such testing levels can be sustained, the Government appears likely to have the base from which to embark on automated contact tracing by the use of an Application (App) on our mobile telephones. On 3rd May, Grant Shapps MP, Secretary of State for Transport, announced on the Andrew Marr Show that an NHS App for contact tracing would be trialled in the week beginning 4th May in the Isle of Wight.

Under the scheme, individuals hand over personal data from their mobile phones to a central database via the App, so that the hub can learn who has been infected and then inform those who have been in recent contact with the infected person, again via the App. The App will gather significant amounts of sensitive data and deploy that to communicate sensitive messages. What can government do with the data, and what should it not do with the data? This paper is directed towards providing an answer to that question. In doing so, it draws on a range of other research papers that have addressed both the technical and legal implications of the App. This Paper attempts to reflect on their insights and propose a route forward from their concerns.

To give, automatically and regularly, such personal information to the State, or even to a software company such as Apple or Google, is an unprecedented increase in overt digital surveillance. We agree that it may be justified if the contact tracing it enables is effective in leading the fight against this disease. But that agreement is conditional – that the information is not misused by government or anyone else and that there are time limits imposed on how long such a scheme should continue. In this paper we consider how those conditions may be met.

In doing so, we are conscious that technology allows ever more ubiquitous overt surveillance. Thermal imaging cameras may be used to monitor public transport users for signs of infection and facial mapping analysis may be used to identify people from those video camera feeds, for example. Such technology is already in use in a number of countries.[1]

Furthermore, advancing AI technology allows large amounts of data to be analysed in order to connect disparate pieces of information from which sophisticated pictures of an individual's activity may be identified even where discrete pieces of data may be considered anonymous. This use of overt surveillance by the State presents considerable dangers for privacy, for State coercion and for misuse. The contact tracing App will be a test of whether a balance can be struck between the legitimate aims underlying its introduction and the rights and liberties of individual citizens. It is important to get it right now because of the precedent it creates for the future.

Finally, data is easily communicated across borders. That creates concerns for the storage of the data and its further use. It will be important that the balance that the UK strikes between legitimate aims of the State in surveillance and the rights of individuals is not undermined by the transfer of the data outside the UK. That requires co-ordination with other States.

---

[1] www.bbc.co.uk/news/av/world-asia-52104798/coronavirus-how-china-s-using-surveillance-to-tackle-outbreak

## THE LEGAL AND PARLIAMENTARY BACKGROUND: NO SCRUTINY TO DATE

At the outset, we make two important points that frame the rest of our Paper:

- There is no legislation specifically designed to regulate contact tracing and future developments of contact tracing.
- The scheme is being introduced without so much as a Green Paper to discuss its ramifications: there has been no consultation process and no scrutiny by Parliament

No *specific* legislation to govern the operation of the App is currently proposed. The public will be dependent on the application of existing laws, principally the provisions of the Data Protection Act 2018, ('DPA 2018').[2] While this Act addresses some aspects of the capture and processing of sensitive personal data and appears to permit an App of the kind proposed, we consider it has limitations on the restrictions and scrutiny it requires. Notably, there is presently in process a data protection impact assessment (DPIA), which is referred to by Dr Ian Levy of the National Cyber Security Centre at GCHQ in the blog that we address in detail below.

Even before considering the outcome of the DPIA, our concern is that the App is managed transparently and in a way which is easily understood and the DPA 2018 does not guarantee that. Yet it is essential. This is not just as a matter of legal nicety. The scheme proposed is a voluntary scheme. As we discuss below, to be effective as a tool for contact tracing requires substantial take-up of the App by the public. Such take-up in sufficient numbers will only be forthcoming if there is complete trust and confidence.

That will be particularly difficult to obtain where, as here, the scheme is being introduced in a rush (so far as the general public is concerned) – although it has obviously been in gestation for a while. There has been no prior public discussion or parliamentary debate. It is of critical importance that such discussion and debate is now conducted. Again, this is not just because of the principle that such far-reaching invasions of privacy should be reviewed by Parliament before being permitted but because it will encourage the necessary trust from the public.

We have no doubt that, both to frame the Parliamentary review and to create the necessary framework of transparency, some more specific legislation is needed, we suggest by amendment of the Coronavirus Act 2020. Such legislative changes as we advocate need not, and should not, however delay the implementation of the implementation of the scheme. We will explain below what we have in mind.

[2] Reading what the European Data Protection Board has said, a centralised contact tracing scheme is permissible, provided it remains consistent with the necessary data protection requirements of Art. 25 (1) of GDPR, which requires data controllers to "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation." See, EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

## UNDERSTANDING CONTACT TRACING

### Two models

There are essentially two models of contact tracing (the second of which comes in two forms):

1. Manual tracing

This relies on people volunteering the information. This is limited because it relies on a conscious decision by the volunteer to inform the powers that be that he/she has or may have become infected, and then on the accuracy of that volunteer's memory. It is also resource intensive because it requires people to investigate and follow up.

2. Automated contact tracing

This is either a centralised or a decentralised system. In both these systems, individuals have Apps on their phones. And, in both, the alerts are sent anonymously, so that the recipient does not know whose infection has triggered the alert, only that he or she has been in contact with someone who is infectious. The important difference between the two systems is whether the data that is collected is stored centrally or on the phone, and who has access to that data:

The decentralised model: all matching takes place on each person's phone and not centrally. Such a system limits the ability of either the authorities or a malicious actor (hacker) to use the computer server logs to track specific individuals and to identify social interactions. This model was proposed by Apple and Google.

It works in this way. The App builds a memory of proximity of the individual's contacts. When two people (A and B) meet their phones exchange a keycode. When A becomes infected, he updates his status in the App and gives his consent to share his key with the database. By reason of the App, B's phone, and that of anyone else who is using the App and who has been in contact, regularly downloads the database automatically to check for matching codes. It then alerts B that somebody he has been near/in contact has tested positive.

The centralised model: under this system, the App updates a central server with the contacts of the phone user. The information that someone (A) has become infected is passed to the centre which then sends out alerts to all contacts (B and others). The central system informs B that they are at risk and advises them to go into quarantine and/or get tested. This is the model that has been proposed for adoption in the UK.

### NHSX – a centralised model

Our understanding is that under the centralised system proposed by NHSX the central server will have uploaded the users' proximity contacts, where matches are made and then sent to relevant phones. It is said that a significant advantage of the centralised architecture is that the NHS thereby gains a reasonably complete picture of the spread of COVID-19 among those who are using the App. In this way, the dataset charts all interactions between all such people. So, it can be used not only to notify individuals that they are infected or at risk of infection and should take appropriate precautions, but importantly to track its spread throughout the nation.

Details as to the proposed operation of the NHS App are given by Dr Ian Levy, of the National Cyber Security Centre, in his recent blog post (4th May 2020):[3] *The Security Behind the NHS Contact Tracing App*.

There he explains that "given the epidemiological model the NHS is using to manage the coronavirus spread in the UK, the fully decentralised model just doesn't seem to work". If that is correct, then there really is no sensible alternative to using a centralised system. Dr Levy tells us that the epidemiological models show that any delay in isolating people who are showing symptoms has a real effect on the spread of the virus. The less delay there is the better the NHS can manage its

[3] www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app We recommend this post to all readers who want to understand more fully what are said to be the advantages of the NHSX centralised model.

spread. This model he says is the best model they have been able to develop at present.

There are downsides to a centralised system which are identified in the blog. Thus, the system ends up with a list of devices that have been near each other, even though they are anonymous. It knows that two devices were near each other on a set of dates (assuming one of them has reported the contacts). In theory, he points out that brings a risk to our privacy. But it is only stored on the NHS App system. Further, he says, there is no way in which a device can be linked to a particular person or a particular place. If an outsider discovers the identity of a particular phone App, he acknowledges that there are theoretical things which that outsider can do to try to understand who the contacts of its owner are, if the outsider has been following that individual. But, as he points out, if the outsider has been following the individual around, he has probably seen who the individual's contacts are anyway. He asserts that this sort of attack cannot be mounted remotely and so it does not scale up into a major risk.

Dr Levy also points out that the system is likely to evolve as NHSX gets more information about the operation of the App. He says that this will provide the opportunity to enhance protections.

### Effectiveness in operation

For automated contact tracing by App to be effective it relies on widespread use of the App and, just as importantly, on accurate testing. The former is necessary to ensure that sufficient capture and dissemination of contact information. Adoption and use of the App will also be dependent on ease of installation and use. The latter is vital to ensure that the message of infection is accurate and credible. As Rafe Jennings points out in his blog on 1st May[4]:

> "…any use of contact tracing Apps is reliant upon widespread availability of testing. To limit false positives, which could spread quickly through a contact tracing system, positive diagnoses of coronavirus would have to come from sanctioned tests. As the government's testing program remains fairly limited in extent, the use of contact tracing Apps and their privacy limitations remains fairly theoretical. If as much as 40% of the population downloaded the App, for any given encounter there would only be a 16% chance that both people would have the App and therefore benefit from digital contact tracing. It therefore remains to be seen how useful digital contact tracing will be compared to traditional contact tracing methods – simply asking people who they'd been in contact with."

Concerns have, however, been raised as to the effectiveness of any App. As a helpful article by Leo Kelion[5] pointed out there are real practical issues with a system, such as is proposed, that is dependent on Bluetooth signals to detect contact matches. These do not show where the close encounter has occurred but simply the fact that it occurred. But such a system is less than perfect because:

- There is a considerable danger of missed contacts and also of false contacts: some phones detect Bluetooth signals from up to 30m away without being able to determine the distance. Yet, interference can prevent two phones noticing each other even when they are within two metres.
- Digital contact tracing will be less able to control for variations such as ventilation, direction of wind or environment – factors which are normally central to manual contact-tracing efforts.
- Digital contact tracing is vulnerable to all forms of fraud and abuse – people who use multiple devices, for example, false reports of infection, and denial of service attacks by adversarial actors.
- In the United Kingdom, 12% of active smart phones are incompatible and a significant number of people have more basic mobile phones with no access to the iOS/Android App stores.

[4] https://ukhumanrightsblog.com/2020/05/01/what-are-the-data-privacy-considerations-of-contact-tracing-Apps

[5] BBC website, 20 April 2020 www.bbc.co.uk/news/technology-52353720

However, Dr Levy attempts to put those concerns to rest in his blog post. He writes that the NHSX App development team have ensured that the App:

- runs well on the supported devices, including quite old ones;
- uses only software development tools and mechanisms that are supported by Apple and Google (as part of iOS and Android development);
- will not drain the battery;
- lets other Apps continue to work properly;
- strongly protects privacy and security of the user; while (most importantly)
- providing the insights which the public health professionals need better to manage the virus in the UK.

We hope that Dr Levy is right, because an App that does not provide reliable information about the spread of the virus, or which routinely indicates the need to self-isolate on the basis of a false identification of a connection, would not justify the huge invasion of privacy that is involved. The rest of this Paper proceeds on the assumption that he is right.

### The merits of a contact tracing scheme

In making that assumption, we anticipate that the systems will have merits even with certain technical limitations. That is because, (citing the Oxford University Big Data Institute[6]), even if false and missed alerts are common, the spread of the virus will still be slowed and people have to spend less time in lockdown or quarantine. Further and importantly, the assessment of the merits does not come in a vacuum. The App must be assessed against alternatives to automatic tracing for controlling the virus' spread.

In *Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease us Out of Lockdown*[7] Professor Christophe Fraser, senior author of the latest report from Oxford University's Nuffield Department of Medicine, explains:

> "We need strategies to exit from the lockdown whilst minimising the risk of resurgence. Combined with other interventions such as community testing and continued shielding of vulnerable individuals, digital contact tracing can help prevent coronavirus from rapidly re-emerging. We hope these latest findings will provide valuable evidence that mobile contact tracing can be carefully deployed after consideration of key epidemiological parameters, combined with critical ethical principles, to ensure we can save lives, reduce the number of people who need to remain in self-isolation, and support as many people as possible to safely and responsibly start returning to active life again. Our models show we can stop the epidemic if approximately 60% of the whole population use the app and adhere to the app's recommendations. Lower numbers of app users will also have a positive effect; we estimate that one infection will be averted for every one to two users."

The European Data Protection Board in its latest guidelines[8] also comes down in favour of contact tracing provided it is managed and conducted properly.

---

[6] www.bdi.ox.ac.uk/news/digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

[7] Op. cit.

[8] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

> "48 The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the 'ratchet effect'. It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation.
>
> 49 The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for health management purposes"

It appears that there is no certain cure for COVID-19 nor any effective vaccine against it on the immediate horizon. In that context we have no doubt that contact tracing by App has merit and subject to proper safeguards should be implemented. The factors that influence that conclusion are set out by the authors of a recent comprehensive paper *Exiting Lockdown: Using Digital Contact Tracing to Defeat Covid – 19*. As they point out[9]:

- a rollout of vaccine is 12 to 18 months away;
- 'herd immunity' will not be achieved quickly and the virus is likely to re-emerge in a peripatetic fashion for years to come;
- social distancing curtails freedoms and severely so if stringently applied. The merits of testing and contact tracing as an alternative that does not involve the direct curtailment of liberties at the price of some loss of privacy become significantly more important;
- contact tracing can help quash existing and prevent future outbreaks, if it is effectively employed;
- but the introduction of Big Data acquired by the UK government through such an App raises profound ethical, legal and operational questions.

In short there is a trade-off which the public must be persuaded to accept if we are to end the present lockdown and to be rid of the impossible economic and social burdens currently imposed to protect us. But that trade-off must be strictly controlled and not abused.

[9] Richard Walton and Julie Marionneau, Policy Exchange, April 2020, https://policyexchange.org.uk/publication/exiting-lockdown

## PRIVACY IMPLICATIONS IN PRACTICE

Whatever we think of the merits of using a centralised or decentralised system (and there are data protection issues with both), it appears that the Government has decided to opt for a centralised system. It is this which we discuss. In doing so we note that the latest information about what other European countries are doing, shows a mixed picture. The French and Norwegian governments are also said[10] to favour centralised contact tracing. France, it seems, will store all relevant data on a central server. But we note that Switzerland[11] is said to be going down a much more decentralised privacy-focused route. Further, Germany which had favoured a centralised approach announced on 26th April that it has switched from that to a decentralised approach[12].

Those interested in this topic will want to see how the two systems work in practice and what issues arise with the competing philosophies.

We turn then to consider in more detail what Dr Levy of the NCSC (at GCHQ) wrote in the blog post referred to in opening above. Dr Levy asserts that the centralised model to be used strongly protects our security and privacy.[13] While we might wish to take that assurance at face value, *in our view it is important that it can be tested and verified by independent means*. For example, Dr Levy says that the NHS team have worked to ensure that:

- The App does not have any personal information about you, it does not collect your location, and the design works hard to ensure that you cannot work out who has become symptomatic.

[10] www.ft.com/content/10f87eb3-87f9-46ea-88ab-8706adefe72d

[11] www.swissinfo.ch/eng/digital-solution_contact-tracing-app-could-be-launched-in-switzerland-within-weeks/45706296

[12] https://uk.reuters.com/article/uk-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUKKCN22807X

[13] Again, Dr Levy's Blog Post should be reviewed in detail because of the careful explanation of the nature of the data captured and the extent to which it is considered to pose a risk of deliberate or inadvertent invasion of privacy.

These are important safeguards, but it is to be noted that it is not always possible to anticipate how data may be correlated so as to derive identifiable information. Dr Levy also says that:

- The design makes sure that it is hard to use the app to track you by being physically close to you – although, Dr Levy writes, there are balances to be struck.

We are unclear what is the balance that is being struck. At present we do not know what the factors weighing in those balances are or how the balance has been struck. Is it the balance between the effectiveness of the contact tracing aspect versus the prevention of physical tracking or some other matters? Whatever it is we need to know. That is a matter which must be explained properly and openly. It should be capable of verification by an independent body.

- The back-end (i.e. the central server) he says is built to be as secure as is practical. He adds by way of reassurance that it holds only anonymous data and will communicate to other NHS systems through privacy preserving gateways. In this way, he says data in the App data cannot be linked to other data which the NHS holds.

Again, this is reassuring but history suggests that even secured databases are the subject of leaks. That is particularly so where they are the subject of deliberate attack and a database of this kind is plainly an attractive target given the wealth of information that it would contain.

At the same time, we feel it is not sufficient to rely simply on assurances such as Dr Levy's. The existing statutory framework, the DPA 2018, does not provide an adequate route to testing and verification. We explain below our specific concerns and what we think must be done.

### The Information Commissioner's position

On 17th April, The Information Commissioner published her opinion on the Apple-Google joint initiative for a decentralised system[14]. She has yet to publish an opinion on the NHSX centralised system. But her spokesman, on 24th April said:

> "People must have trust and confidence in the way personal data is used to respond to the COVID-19 crisis. The ICO also recognises the vital role that data can play in tracking the pandemic and the need to act urgently. We have been working with NHSX to help them ensure a high level of transparency in governance. We will continue to offer that support during the life of the App as it is developed, rolled out and when it is no longer needed."

We agree completely.

In her opinion on the Apple-Google initiative, she had noted that it would be possible for those developing COVID-19 tracing Apps to design Apps that collect other data and use other techniques beyond those initially envisaged, i.e. mission creep or worse, overreach or even abuse.

As the Commissioner reminded us in her opinion, organisations designing contact tracing Apps (which of course includes NHSX) are responsible for ensuring any App complies with data protection law where they process personal data. Further, where such organisations are the controllers of that data, the controller must ensure that it assesses the data protection implications of all processing and ensure that the processing is fair and lawful. She emphasised (rightly) that from the public's point of view it is crucial that the processing is transparent. That was said in the context of the decentralised system.

The Commissioner noted the vital importance of developing contact tracing solutions subject to data protection compliance and good practice but stressed that they must espouse robust security (including the use of encryption and covering each stage of the data processing). She stressed the importance of data minimisation, transparency and user control.

[14] https://ico.org.uk/media/about-the-ico/documents/2617653/Apple-google-api-opinion-final-april-2020.pdf

In our view, any supporting technology, including centralised processing to support contact tracing, should follow the same principles. Those principles apply with at least equal if not more force to the centralised system proposed.

**Conclusion**

Accordingly, we suggest that our analysis makes necessary the establishment of an independent body for audit and review. Such a body, *the Testing and Tracing Command Centre [TTCC]*, has been proposed by Policy Exchange in a paper to which we refer next.

## USE OF THE APP MUST BE VOLUNTARY: THE NEED FOR TRUST

The Policy Exchange paper's[15] authors concluded that making the App compulsory will be counter-productive and do more harm than good to British society. It will legitimise fears of a "surveillance state" and unnecessarily alienate that part of the public which is wedded to personal privacy. So, if it is to be a voluntary system and taken up by a sufficiently large number of the population, government must provide transparent reassurances on how the data will be stored, analysed and used. High levels of trust will be vital to getting a critical mass of people to subscribe to the App and to use it routinely. Its use should be time-limited and not indefinite. Finally, legislation (to amend the Coronavirus Act 2020) should be introduced to incorporate safeguards specific to contact tracing. We summarise such safeguards below. In short, the UK public will need to be convinced that the price of giving up some privacy is one worth paying to secure freedom. Finally, a public debate on this issue is necessary to assist understanding.

We agree with all that.

[15] Richard Wilson and Julie Marionneau, Policy Exchange, April 2020, (which we have cited above) thttps://policyexchange.org.uk/publication/exiting-lockdown

## SCRUTINY – OR LACK THEREOF

A central concern that should immediately strike anyone considering this issue is the risk of central government making improper use of the information it holds. Could it be used for expanded purposes? Could it be the first step to "Big Brother" sending a text to individuals ordering them on pain of penalty to self-quarantine? We do not wish to be alarmist, but it is important that we all grasp clearly how such a system could develop.

Difficult times are always said to require difficult measures. We would do well to look back to 2005 and the aftermath of terrorist attacks including the atrocity on public transport on 7th July that year. That was when the Blair government proposed that the police should have power to detain suspected terrorists for up to 42 days before bringing them to court. Parliament rightly, as the subsequent 15 years have shown, took the view that that was excessive and unnecessary. But at the time terrorism was a real threat, as it still is, and well-intentioned persons in authority concerned to protect their citizens thought that 42 days detention was a necessary and proportionate response to the threat.

At the present time, Parliament is barely sitting. It is likely that there will be constraints for some time to come on the effectiveness with which Parliament can operate. That has important implications for the degree of scrutiny which will be given to the measures proposed or their possible extension.

There has been no Green Paper or other consultation process properly explaining in detail how the centralised system is to operate and what boundaries will be placed on it. To whom will NHSX answer?

### Important considerations for Parliament

At the same time that there has been no scrutiny of the App to date and limited capacity for scrutiny going forward, there are important considerations for Parliament that cannot be answered by existing legislation:

- Should it be made obligatory to carry personal devices capable of installing the App? Or at least obligatory in respect of those who have capable device, but who fail to carry them or install or run the App?
- Should there be sanctions for failing to install the App or to use it once installed?
- Could it ever be permissible to re-purpose or to share personal data derived from any symptom tracking and contact tracing App?

  The answers to all these questions must – in our opinion – be a firm, "no". But they are political questions that demand debate. In that regard, we draw attention to the fact that in Australia, the Biosecurity Determination Act 2020, which was passed to coincide with their national contact tracing App, COVIDsafe, appears to reflect our opinion. That Act provides:

"(2) A person must not:

(a) refuse to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or

(b) take adverse action (within the meaning of the *Fair Work Act 2009)* against another person; or

(c) refuse to allow another person to enter premises; or

(d) refuse to allow another person to participate in an activity; or

(e) refuse to receive goods or services from another person; or

(f) refuse to provide goods or services to another person; on the ground that, or on grounds that include the ground that, the other person:

(g) has not downloaded COVIDSafe to a mobile telecommunications device; or

(h) does not have COVIDSafe in operation on a mobile telecommunications device,

(i) has not consented to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store."

The Biosecurity Determination 2020 states that the purpose of the statute (emphasis added), "is to make contact tracing faster and more effective **by encouraging public acceptance and uptake of COVIDSafe**". The Australian Act and the use of a contact tracing App raise issues which the authors of the Data Protection Act 2018 did not have in mind. We can see that if take-up is too low and the present emergency remains intractable, there might be pressure to make it in effect compulsory to use the App by disproportionately disadvantaging those who do not. We think that would do more harm than good and would be likely to undermine trust and confidence.

If there are to be such provisions in the UK then they must be given the force of law. The Coronavirus Act 2020 could and should be amended to include provisions of similar effect. Amendment to the Coronavirus Act would make it plain that the provisions being incorporated applied only to COVID-19 and not to general protection of the public health. That would be a means of preventing overreach.

## THE PROPER APPROACH GOING FORWARD

In the light of the matters set out above, in our opinion, the following points arise as a way of moving matters forward:

- Government must make it absolutely plain that the implementation of the system will not be subject to overreach or mission creep. It must only continue for as long as is strictly necessary. We favour a review mechanism after six months and a sunset clause, at the least, running in tandem with that in the Coronavirus Act 2020. Public trust is essential.

- Legislation should be enacted that makes it clear:

  – Data must be kept completely confidential.

  – Data must not be held forever.

  – Personal data of an individual (including location data) must never be made public, must never go beyond the institution which is collecting it and must be destroyed in due course after a set period.

  – There must be no possibility that the NHS sees commercial opportunity in selling even anonymized data obtained through the App for use by others with Artificial Intelligence – the potential of misuse of data mining can never be underestimated.

  – There must be stringent protection against malicious actors interfering either in the operation itself of the App or in accessing the data then held by NHSX.

- There must be proper oversight of the whole process. We favour the creation of a new institution such as recommended by Policy Exchange in the paper referred to above and which we commend to all readers of this paper. That is a **Testing and Tracing Command Centre [TTCC]**. This will have the specific task of overseeing and implementing the national testing and tracing strategy for hunting down and defeating COVID-19.
- There must be judicial oversight of the TTCC.
- The Coronavirus Act 2020 should be amended as soon as practical so as to give effect to the above and incorporate safeguards comparable to the Australian legislation. Such amended legislation should address the establishment of the TTCC and judicial oversight of it.

## CONCLUSION

In concluding, we remind readers of the powerful analysis by David Anderson QC[16] (now Lord Anderson) in 2015, *A Question of Trust*. Chapter 2 of that paper explains the concept of privacy and why it is important to the well-being of each individual and society as a whole. The protection of privacy is an important goal, we should not allow the understandable immediate demands of addressing the COVID-19 crisis to obscure that goal.

If, but only if, there is swift and effective action to procure the involvement of Parliament and implement the measures we propose above, the Government may be able to establish the necessary trust to generate sufficient take-up of the App for it to be an effective tool in defeating this ghastly virus while protecting fundamental rights. It will then be a powerful tool to help speed up the process by which social distancing and other enforcement measures can be relaxed.

[16] Then the Independent Reviewer of Terrorism Legislation

Lord Sandhurst QC
Benet Brandreth QC
Simon PG Murray

London
6th May 2020

For further information on the Society of Conservative Lawyers contact:
The Administrative Secretary, The Lodge, Deaks Lane, Cuckfield RH17 5JB
administrator@conservativelawyers.com
www:conservativelawyers.com



May 2020