Contract tracing: one step closer to Big Brother?

The Government confirmed at the beginning of May that a new contact-tracing app for managing the coronavirus outbreak would be piloted on the Isle of Wight. The purpose of the app is to alert users if they have been close to someone with the COVID-19 virus. The app will, reportedly, use Bluetooth technology to register a 'contact' when people come within 6 ft of each other for at least 15 minutes. If someone develops symptoms akin to the COVID-19 virus, they inform the app and an alert will be sent to other people they have been in close contact with. The user who experiences symptoms and alerts the app will then be offered a test.

Once the Isle of Wight trial is complete, the app will be referred back to NHS digital for further assessment. There are reports that the app has so far failed the tests needed to be included in the NHS app library, including cyber security, performance and clinical safety. It was reported that as of 14 May, just over half of the island's 140,000 residents (reportedly 72,300) had downloaded the app. The app developers have said it must be downloaded and used by 60 per cent of Britons if it is to prove effective. The early reports suggest the app's usage has not met this target during its testing on the Isle of Wight. It is envisaged that the app will form part of the Government's contract tracing system, which is due to launch on 28 May 2020.

What is contract tracing?

Contact tracing is a system used to slow the spread of infectious diseases like coronavirus. It has already been used in places like Hong Kong, Singapore and Germany. It usually involves asking coronavirus patients to list all the people with whom they've recently been in prolonged contact. Those people will then be tracked down and potentially asked to self-isolate. This is sometimes complemented by a location-tracking mobile app, which monitors when users come into contact with each other.

Naturally, like with any app that tracks our movements and records our data, concerns regarding the app's privacy and information governance have been discussed nationally. This approach involves the transmission by a central server of random identifiers by an individual's smartphone. What follows is that other smartphones in proximity to the individual's phone recognise the identifiers and transmit this information back to the central server. In the event of an individual testing positive for COVID-19, the identifiers that their phone has received from other phones can be loaded together with the times and duration of contact.

While a centralised design would share data directly with public health professionals that ***may*** aid in their manual contact tracing efforts, the NHS's decision to pursue an approach that provides a tool to identify and reach out to other potentially infected people has been criticised by internet experts. Alan Davidson and Marshall Erwin of the non-for-profit Internet organisation Mozilla, have said that the Government's current approach is problematic because it expands government access to what is known as the "social graph", this being data about an individual, the individual's relationships and links with others. Since

the pilot launched, it has been found that app does indeed have security flaws, which include weaknesses in the registration process that could allow attackers to steal encryption keys, (which would allow them to prevent users being notified if a contact tested positive for Covid-19 and/or generate spoof transmissions to create logs of bogus contact events) and the storing of unencrypted data on handsets that could potentially be used by law enforcement agencies to determine when two or more people met.

The alternative to a centralised approach would be a decentralised model. The feature of this model is that identifiers are generated on an individual's device and cannot be matched by any central server. When an individual is diagnosed positive for COVID-19, they tell the system that they are ill and give no extra information. The system periodically collects a list of everyone who has said they're ill and sends it out to all users of the app. Individual devices look to see if any of its local contacts are on the list. This model ensures that the proximity of persons to COVID-19 patients is not known to any central server or authority.

Decentralised approach - why did the NHS reject this approach?

Tech giants such as Apple and Google have agreed to partner on developing contract tracing technology. Their advice to governments was to build contact-tracing apps that operate in a decentralised way, allowing individuals to know when they've been in contact with an infected person but preventing governments from using that data to build a picture of population movements in aggregate. Crucially, under their model a public health authority cannot ask a phone to gather a list of every other phone it has been in contact with. The reason for this? During a press call to journalists on 14 April, Google said the limits the partners have implemented are because neither company wanted their operating systems to be abused for draconian surveillance efforts. Experts observe that in order for any app to be successful, it needs to work on the devices we currently use and for that, we will need the manufacturers to agree and lift their technical restrictions to allow the app to work in the background. If not, states will effectively need to adhere to the manufacturer's standard of privacy for their operating systems. Apple have said that the standard of privacy that they are demanding is a decentralised system. Given that over 51% of smartphone users in the UK use iPhone, the prospects of a successful centralized tracing app are limited. By pursuing a centralised model, the NHS may not be able to obtain reliable data as it will likely become difficult to get iPhones to work with the model, without a workaround that will just stop people using the app. It has been reported that Switzerland became the first country to launch a contract tracing app that incorporates Apple and Google's technology.

The applicable legal framework

The Health Secretary, Matt Hancock has said that "[A]*ll data will be handled according to the highest ethical and security standards, and would only be used for NHS care and research. And we won't hold it any longer than is needed*". The Health Secretary will of course be aware that any tracing app model is also subject to the UK's data protection legislation, including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR), as well as the right to privacy guaranteed by Article 8 of the European Convention of Human Right (ECHR),

ECHR

Article 8 of the ECHR provides everyone a qualified right to respect for their private and family life, home and correspondence. The European Court of Human Rights has identified private life as including the physical and psychological integrity of a person, gender identification, name, sexual orientation & sexual life and crucially for the purpose of the app, health data.

Article 8 is a qualified right rather than an absolute right. This means that interferences with the right may be justified. The ECHR provides the framework to justify any interferences with the right. Firstly, any interference must be in accordance with the law, secondly it must pursue a legitimate aim and thirdly, it must be necessary in a democratic society in the interests of public safety or economic well-being of the country & the protection of health (there are several reasons however these are the two that are applicable to the facts).

The European Court of Human Rights has repeatedly affirmed that any interference by a public authority with an individual's right to respect for private life and correspondence must be in accordance with the law. The Department of Health and Social Care, NHS England and NHSx, the innovation unit behind the app, would fall within the definition of public authority given NHSx is performing a task carried out in the public interest or in the exercise of official authority vested in it. This is the definition used in the Freedom of Information Act 2000 and adopted in the Data Protection Act 2018. The GDPR does not define a public authority.

For an interference to be in accordance with the law, any legislation which must be clear, foreseeable and adequately accessible. No legislation has been introduced for the creation of the app but such a method of processing data will need to be compliant with the legal framework set out in data protection legislation. Additionally a restriction on a Convention right cannot be regarded as "necessary in a democratic society" unless it is proportionate to the legitimate aim pursued. Contracting States to the Convention are afforded a margin of appreciation in respect of this but ultimately, it is the duty of the State to demonstrate the existence of a pressing social need behind the interference. Inevitably any State relying on a justification for interference will refer to the effects the COVID-19 virus is having on public health but also the effect on a country's economy, which is applicable to the UK given the reports the country's economy faces a long and slow recovery from the impact of the crisis. The impact assessment, the details of which are set out below, contains the following statement, "*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*."

GDPR/DPA

As set out above, any method of processing data will need to be compliant with the legal framework for data processing set out in the DPA 2018 and GDPR.

The GDPR requires the following for the processing of any data (Article 5):

- to have been done lawfully, fairly and in a transparent manner;
- personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller, this likely being the NHS, shall prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Article 35). This is commonly known as a data protection impact assessment ("DPIA"). Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, then the GDPR requires the controller to consult with the supervisory authority, which in this country is the Information Commissioner's Office ("ICO"). Notably the ICO took the view that the Apple-Google proposal aligned with the principles of data protection by design and by default.

The DPIA for the NHS app was published on 6 May 2020. It stated:

- that the collection of data is always done voluntarily but it does not admit that this is not true, given the app works by other people uploading information about you, including third parties you were in the vicinity of;
- there is a blanket refusal to deny the right to erasure (Article 17, GDPR) but there is no lawful basis on which the blanket refusal relies on;
- the ICO will only be briefed about the proposed processing, not consulted which is what Article 36 of the GDPR requires if the DPIA indicates that processing will result in a high risk; and
- the risks identified with processing data are redacted so it is not possible to see what these are, although security risks have been reported. It is not clear if the risks are such that NHSx now have to consult with the ICO.

Lawyers instructed by the Open Society Foundation have correctly pointed out the following issues with the Government's model including:

- That the data sharing arrangements that the Government has announced for the creation of a data store for purposes relating to the COVID-19 pandemic currently lack sufficient clarity and detail to comply with the data protection principles set out in Article 5 GDPR;
- That the Government has not provided sufficient information to explain how data sharing arrangements will comply with the guidelines in the Draft Data Sharing Code of Practice published by the Information Commissioner's Office ("ICO"). The Code, reflecting the

requirements of the GDPR, requires (amongst other things) that a data sharing arrangement is in place to prescribe (i) the purposes of data sharing; (ii) the respective roles of the parties and their access to the data concerned; and (iii) the procedures to allow data subjects to realise their rights under the GDPR and the DPA.

Most concerning is that the lawyers suggest a centralised and mandatory system, if combined with other data, would potentially provide the Government with a wholly unprecedented level of data about the social network of the majority of the population and that in the current climate of a serious pandemic, they believe such interference would require an equally 'unprecedented level of evidential justification' to meet legal requirements and ensure public confidence. In a society still reeling from the revelations concerning Cambridge Anayltica, critics are right to be wary of the measures the Government are taking. Various civil society organisations, privacy advocates and academic researchers including Liberty, Big Brother Watch and Privacy International have since written to Matt Hancock MP to express concerns about the plans to build such a data store.

Another organisation, Open Rights Group have signaled their intent to bring a legal challenge to the Government's programme as whole. While a DPIA has been carried out on the app, it appears no such assessment was carried out on the entire programme before its launch on 29 May 2020.

It is unknown whether use of the app will be mandatory or voluntary. The language used by Health Secretary on BBC Breakfast on 5 May 2020 suggested there was a duty for those downloading the app in that it would help save lives. Such language implies there will be an obligation to participate. Since then, in his press conference on 27 May 2020, Matt Hancock appears to have revised the guidance, "it is your civic duty, This will be voluntary at first because we trust everyone to do the right thing, but we can quickly make it mandatory if that's what it takes". Meanwhile, Matthew Gould, chief executive of NHSx, emphasised that the app was voluntary to download and promised that NHSx would publish both the source code and the data protection arrangements underlying the app. Perhaps another example of why clear guidance is needed from the Government.

The privacy notice

As the test and trace system is about to be launched, we are now able to review the privacy notice, which is quite revealing. It uses US language such as 'personal identifiable information' rather than 'personal data', which is the language used by the UK GDPR and DPA. Why would the privacy notice use the American terms? The information the App acquires and its continued retention is treated as processing under the GDPR. NHSx is therefore obliged to comply with the provisions of the GDPR so you would expect the privacy notice to use language consistent with the legislation.

Most concerning is that the notice states 'personal identifiable information' collected by the NHS Test and Trace on people with coronavirus or who have symptoms will be kept for 20 years. The law requires personal data to be kept for no longer than is necessary. Is the Government expecting the pandemic to last 20 years?

Of course the data being processed is not just any data, it is special category data as it concerns health (Article 9). In the DPIA, the Government state the legal basis for processing special category data is that it is necessary for health or social care purposes (Article 9(2)(h), underpinned by Schedule 1, Part 1, s. 2(2)(f) of the DPA 2018. Additionally the Government states the processing is necessary for public health, with the required basis in law being Regulation 3(1) and 3(3) of the Health Service (Control of Patient Information Regulations) 2002.

Further concern is raised because the privacy notice does not specify who has access to the data only that "it can only be seen by those who have a specific and legitimate role in the response and who are working on the NHS Test and Trace." That is a broad and is likely to include various private technology companies the government has enlisted to build data stores for the app, as suggested by reports.

Parlimentary criticism

Since the Government announced on 5 May 2020 that the app would be piloted on the Isle of Wight, the Joint Committee on Human Rights has published a Report on the contact tracing app, concluding that if effective, the app could pave the way out of the current lockdown restrictions and help prevent the spread of Coronavirus, but there are significant concerns regarding surveillance and the impact on other human rights which must be addressed first. On the other hand, the Committee have observed that "*Digital contact tracing will not be as effective if uptake is low. Uptake will be lower without user confidence in privacy protections—therefore robust privacy protections are themselves key to effectiveness of the app and the digital contact tracing system*."

As part of their recommendations, the Committee have suggested a contact tracing app must not be released unless strong protections are in place and there are guarantees on the following:

- Efficacy and proportionality: efficacy must be clear and if not, then the benefits of the app and the level of data being collected will be not be justifiable and it will therefore fall foul of data protection law and human rights protections.
- Primary legislation: this must be enacted to guarantee data and human rights protections and accompany any data gathering by the app
- Oversight: An independent body should be established to oversee the use, effectiveness and privacy protections of the app and any data associated with this contact tracing. A Digital Contact Tracing Human Rights Commissioner should be responsible for oversight and they should be able to deal with complaints from the Public and report to Parliament.
- Regular reviews: An undertaking from the Health Secretary to conduct a review every 21 days of the app's efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data.
- Transparency: The Government and health authorities must at all times be transparent about how the app, and data collected through it, is being used.

What about when the pandemic is over? The Health Secretary has repeatedly said that data cannot be retained by the government and can be deleted from the devices. Matthew Gould confirmed to the Human Rights Committee that the data can be deleted as long it is on an individual's own device but once it is uploaded, "*it becomes enmeshed in wider data, and the technical difficulties of deleting it at that point become tricky*". He went onto say that, at the end of the crisis, "*all the data will either be deleted or fully anonymised in line with the law, so that it can be used for research purposes*". As set out above, that is not clear given what is set out in the privacy notice regarding the suggested retention period of 20 years.

You can find the Committee's report on the proposed app here. Harriet Harman MP, who chairs the Parliament's Human Rights Committee, has announced she is seeking permission to introduce a private member's bill to limit who could use data gathered by the app and how and create a watchdog to deal with related complaints from the public. The proposed bill has been dismissed by both the Health Secretary and the Leader of the House of Commons as not being necessary.

While we all have a duty to combat the spread of the virus, the Government and public authorities have a legal duty to ensure our rights and fundamental freedoms are not overridden in the process.

For more information, please contact the authors:

Tamsin Allen

Emily-Jade Defriend

Daniel Shaw