Explainer: NHS Covid-19 Contact Tracing App and Human Rights

A key part of the UK government's plan to slow the spread of Covid-19 is their new contact tracing app.

The NHS app has been developed by NHSX, the digital development side of the NHS. NHSX explains that the app is hoped to "reduc[e] transmission of the virus by alerting people who may have been exposed so they can take action to protect themselves, the people they care about and the NHS."

While the app has potential to really help reduce the spread of Covid-19, there are widespread concerns over the risks to people's privacy if they use the app. For the app to be effective in reducing the spread of Covid-19, the majority of the public need to use it. But to for this to happen, people need to be able to trust the app. Worries about people's privacy must be addressed and protection of privacy must be secured.

What is the app?

The app is developed by NHSX.

It aims to trace the movement of the virus by working out which people infected individuals could have passed the virus onto. People who have the app and have been near a someone who has symptoms of Covid-19 will be alerted and advised to self-isolate. The exact advice on what you should do will depend on the context and how the app develops. The contact tracing app is part of a wider public health strategy responding to Covid-19.

The parliamentary Joint Committee on Human Rights (JCHR) explain what contact tracing means in a bit more detail:

"Contact tracing is one way of trying to control and track the spread of the virus. It involves notifying individuals when they have come into contact with others who may have been exposed to the Covid-19 virus and giving them appropriate advice, for example to get tested and or to self-isolate, in order to minimise the further spread of the virus. Several countries are using smartphones to speed up the process of contact tracing.

Digital contact tracing generally works by an app on a user's smartphone registering and storing details of another smartphone when it is within a defined distance for a certain period of time and if a user tests positive for (or is suspected of having) the virus, the app notifies these contacts that they may themselves be affected."

The Parliamentary Office of Science and Technology have written a really helpful piece on contact tracing apps and how they actually work, and the general issues with getting digital contact tracing to be useful. You can read it here.

There are different approaches to digital contact tracing, and there has been lots of discussion about them recently. These discussions have mainly been on whether the NHS app should take a "centralised" or "decentralised" approach. The current NHSX app uses the centralised model.

This has raised concerns over the storage, collection and sharing of huge amounts of personal data, and how this impacts people's privacy.

Please note the UK government have recently made a U-turn in their approach to the app. Until 17 June 2020, they were developing a centralised app. Now, they have decided to develop a decentralised app instead.

What is a centralised approach?

In centralised models, data are shared with a central database managed by an authority, such as the NHS or the UK government.

Ian Levy, Technical Director of the National Cyber Security Centre, says that in the centralised model, a "user reports their symptoms, but also gives all their anonymous contacts to the public health authority, along with some details about the type of contact they've had (duration and proximity for example)." (Please be aware that Ian Levy and the National Cyber Security Centre strongly backed the development of the centralised app.)

The Parliamentary Office of Science and Technology explains a benefit of this: "[a]n advantage of a centralised system is that anonymised data in the central database could be used for research into the effectiveness of the app and understanding the spread of the virus."

What is a decentralised approach?

With a decentralised app, most data is stored locally on an individual's phone and as little data as possible is shared with the NHS or other authority. This is said to give users more control over their information.

This is thought to be the approach that interferes less with your privacy. It is this approach that the UK government are now exploring, and it will be developed using the Apple/Google framework. This decentralised approach is being used by many other countries across the world.

What does this mean for people?

The app, and digital tracing more generally, could certainly achieve important things. It could be key to learning more about Covid-19 and how it is spread and helping to slow the spread of the virus too. This could be great news for people in the UK, as it could help bring about the end of the widespread lockdowns we've been under since March. With the ability to trace and track the movement of the virus, while some people will be specifically asked to self-isolate, it will hopefully mean that in general, people will be able to have more freedom and that people might not be asked to stay indoors and socially distance indefinitely for too much longer.

But it's also important to remember that the introduction of the app, when it happens, will mark an increase in the collection and storage of personal data, such as your location and your phone contacts, by public bodies. There has been lots of talk about how this could lead to privacy breaches, and people seem to be wary of giving all this information to public bodies.

The app also needs to have a really good uptake amongst the public for it to be effective. If not very many people download and use the app, it won't really be able to trace the virus effectively. You could imagine a situation where one person using the app does develop symptoms, yet no one they were on the bus with the day before, for example, had the app downloaded or running in the background. None of these people who had been near the person who then developed symptoms would even know to self-isolate. And in that case, what was the point in that one person having the app and allowing it to collect and use their personal data? On top of that, not everyone will be able to download or use the app anyway – not everyone has a smartphone, and not all smartphones are able to download the app. As a result, the uptake might not reach the levels needed for the app to be effective.

There are other ways the app might affect people, and we'll discuss some of the human rights concerns below.

Which human rights are involved?

The right to liberty (Article 5 of the HRA)

The right to liberty is not an absolute right, and so it can be restricted in some circumstances. Any restriction of the right to liberty (and any other right) must be authorised by law and it must be lawful, for a legitimate reason set out in the right itself, and importantly it should be proportionate.

The app works by alerting people to the fact that they have been in high risk contact with someone who has Covid-19 symptoms. The JCHR suggest that reporting of symptoms could be done "via self-reporting into the app; by uploading confirmation of an approved test; or health authorities themselves uploading results onto the app server." If the app relies solely on self-reporting of symptoms, this may result in false alerts being issues to be people. This could mean that people are asked to self-isolate for 14 days even when there has been no risk to them, thereby impacting their right to liberty.

The right to respect for private and family life(Article 8 of the HRA)

The key right that the app may pose a threat to is the right to respect of private and family life. This right includes protection of your personal information and data, which could include medical information and location data. This right can be restricted, but again, only if the restriction is lawful, for a legitimate reason set out in the right itself, and proportionate.

The app works by enabling huge, mass sharing of data between people and with the authorities. As a result, it represents a big interference with our private data and information. The authorities have a legitimate reason to restrict our right to private for family life, as set out in the right itself – to protect the right to life, which is threatened by Covid-19, and to protect public safety. However, for the interference of our right to private and family life to be lawful, it must also be proportionate. In this situation, the restriction would only be proportionate if it helped to achieve the aim of reducing the severity of the lockdown and to helping to prevent the spread of Covid-

19. The app and its digital tracing systems must be effective. If not, the collection of huge amounts of data is not proportionate.

Regular monitoring of the efficacy of the app must take place to show that the use of data and interference with people's privacy is proportionate.

It is also important that the data which is collected through the app is only used for the original purpose it was collected for – to help slow the spread of Covid-19. In data protection law, this is called the principle of purpose limitation. If the data is used for any purpose, this would be unlawful and could breach our right to private and family life.

With the UK government's recent U-turn meaning that the NHS app will now follow a decentralised app, there will hopefully be less information sharing with the authorities. While this would be good news for the right to privacy, we don't know much about what the final app will look like, or how it will work exactly. Nonetheless, the important checks and safeguards discussed above are still essential in making sure our rights aren't interfered with unnecessarily.

Other rights

What's more, the lockdowns have already impacted a range of our rights, including the right to liberty, freedom of assembly (which covers the ability to meet in public places and meet with others) and the right to education (which protects our right to an effective education within the UK's existing educational institutions). Please see our handy Explainer on Police Powers and Lockdown (England) for more information.

Getting the balance of rights and restrictions is really important. If the app isn't effective and doesn't help trace the virus, then it won't assist in the easing of lockdown and these rights will continue to be restricted.

The JCHR have discussed the app and its interference with human rights in the context of data protection laws. Please note that their Report was written before the UK government changed course, so when it was still developing a centralised app, which is thought to be the approach which interferes most with our privacy. Please keep this in mind when reading the Report, but there are still really important issues raised which will apply to the app no matter what form it takes.

Contact tracing apps across the UK nations

The Governments in the devolved UK nations have different approaches to the app.

Before the UK government's change in approach, the Scottish Government opted for a system that differs from the NHS contact-tracing app. The Welsh Government had said it would develop their own digital systems and also use the UK government's NHSX Covid-19 app. Northern Ireland's health minister had rejected the UK government's tracing app, and said it was working on a separate app that could share data with the Republic of Ireland.

At the time of writing this Explainer, no further information could be found on the approach in Scotland, Wales and Northern Ireland since the UK government's change in approach to the app, with a decentralised approach now being developed.

What happens now?

For the time being, we can only wait and see how the app develops. As we know more, more detailed discussions can take place on how our human rights may be impacted by the app and its use of data. The Explainer can form the basis of these discussions.

It's important to remember that any interference with our rights must be lawful, for a legitimate reason set out in the right itself, and proportionate. In the case of the NHS app, this means that the app must be effective in helping to slow the spread of Covid-19 and assisting in loosening the lockdown measures.

The JCHR in their Report (written before the UK government changed approach with the app) recommended the introduction of new legislation based on data protection principles which would put legal safeguards on digital contact tracing to protect our rights, and particularly to safeguard children. The UK government rejected the recommendations. In light of the UK government's change in approach to the app, it will be interesting to see if the JCHR make new recommendations for a decentralised app. Whatever form the app eventually takes, its interference with our rights and its access to huge amounts of the public's personal data must be scrutinised.

Where can I find more information?

- For more information on human rights during Covid-19 and the changes to law and policy so far, please see BIHR's useful Coronavirus Hub.
- For NHSX info on the app, please click here.
- To read the UK government's recent announcement on the app, please click here.
- For NHS info on the track and trace approach, please click here.
- For the JCHR's work on the app so far (before the UK government's change in approach), please click here.
- For the Parliamentary Office of Science and Technology's analysis on 'Contact tracing apps for COVID-19' (published before the UK government's change in approach), please click here.

PLEASE NOTE: BIHR Explainers are provided for information purposes. These resources do not constitute legal advice. The law may have changed from the date of writing.