Virus Tracking Apps Will Need To Pass Privacy Law Muster

By **Scott Hopkins and William McConagha** (April 15, 2020, 5:09 PM EDT)

Scott Hopkins

William McConagha

Many countries around the world are being forced to watch as the only tool they have to suppress COVID-19 — social distancing — causes unprecedented damage to their economies. Because suppression measures may be required until a vaccine is available (possibly 12 to 18 months from now), the U.K. and other countries are developing less economically damaging techniques, chiefly systems of testing and contact tracing, similar to those deployed in South Korea, Singapore and China.

In this article, we discuss this technology and consider the data protection and cybersecurity concerns it may raise.

How It Would Work

Mobile Applications

While countries ask individuals to stay home as part of their lockdowns, essential workers continue commuting to their workplaces. For these essential workers, some employers have implemented contact tracing methods in accordance with applicable domestic employment and data protection laws.[1]

Countries such as the U.K. are planning gradual lockdown exit strategies by developing public health care mobile applications that will assist in both the testing and tracing of individuals to enable their return to the workplace but only after certain checks have been cleared. In practice, the government would request that individuals download onto their mobile phone a public health care application and use it to identify themselves and provide certain health-related information, including whether they have been experiencing COVID-19 symptoms, and/or share their temperature reading.

The application would use the information to build health profiles of its users to assess whether or not they need COVID-19 testing. If an individual tests positive, the application would notify both that person and also the individuals with whom the infected person may have come into recent contact based on location information stored by the application and suggest necessary quarantine measures while maintaining the infected person's anonymity. The application would request those notified to undergo testing themselves, repeating the process for any subsequent positive results.

This application could potentially be further developed to request that an individual have their temperature taken (potentially through the application itself) prior to entering a building, such as their workplace. In the case of a high temperature reading, their entry would be blocked and they would be requested to work remotely or be tested. Alternatively, for a normal temperature reading, the application would generate a code (e.g., a color code where green is all clear) enabling the individual to access the building.

Testing Tools

Temperature readings could be supplemented by other self-testing tools currently in development, such as tests that use swabs to look for the virus or antibody tests that look for evidence that the individual has had the virus.

Public Health England is looking to roll out 15-minute home-testing kits that would operate similarly to home pregnancy tests, making use of blood, saliva or urine to provide results. Such tests, reliant on antibody testing, would determine whether COVID-19 antibodies are present in the sample, indicating that the individual has recovered from the virus and gained some degree of immunity to it.

Such tests are currently undergoing trials in the U.K. to determine their accuracy. The home-testing kits have so far not been made publicly available as they have not yet passed evaluations. Professor John Newton, appointed to supervise the testing process by U.K. Health Secretary Matt Hancock, has stated that the 3.5 million home-testing kits the U.K. ordered from China are not accurate enough to be rolled out on a large scale.

In contrast, the U.S. government's approach to developing alternate suppression measures has so far involved a focus on personal protective equipment and fast-tracking COVID-19 testing, including immunity tests. The U.S. Food and Drug Administration's approach to the regulation of these tests has differed substantially based on technology.

Molecular diagnostic tests have been subject to FDA review through the Emergency Use Authorization process, but in an official guidance released on Feb. 29 and updated on March 16, the FDA authorized the commercialization of serology immunity tests without agency review or approval, as long as: (1) the tests are not for home use; (2) the tests are validated; (3) the manufacturer or laboratory has notified the FDA; and (4) certain contextual information is included in the test reports.

The FDA cited the decreased complexity of the serology tests as a reason they can be used during the crisis without approval, stating, "Considering that serology tests are less complex than molecular tests and are solely used to identify antibodies to the virus, [we do] not intend to object to the development and distribution by commercial manufacturers or development and use by laboratories of serology tests to identify antibodies to SARS-CoV-2."

To date, the FDA has not authorized any test — molecular or serology — for home use. But public health experts in the United States are increasingly focused on serology tests as an important tool in the recovery, noting they can be used to identify evidence of immunity in those who have recovered from infection and to help gauge background rates of exposure to inform local and regional decision-making.

Two former FDA commissioners recently extolled the potential of serological assays in a published paper titled "National Coronavirus Response: A Road Map to Reopening," and a reporter for the Washington Post who has been covering the pandemic described the potential of the so-called test-trace-quarantine framework.

U.K. Suppression Methods and the NHSX Application

The National Health Service, the U.K.'s public health care service, is looking at developing an application to help the NHS track and monitor the spread of COVID-19 as part of the U.K.'s strategy for managing the pandemic. Leading these efforts is the innovation arm of the NHS, the NHSX, which sets national policy for the NHS in the field of digital and data technology (including data sharing).

The COVID-19 application is meant to help the U.K. government and the country's health care leaders understand how the disease is spreading and proactively combat infections by diverting patients to the facilities best able to care for them based on demand, resources and staffing capacity. The success of the COVID-19 application will depend largely on whether a sufficient proportion of the U.K. population signs up and uses it in a disciplined manner to enable a safe post-lockdown era in the context of this pandemic.

The NHSX is working with developers to make the COVID-19 application Bluetooth-based. Privacy advocates argue that a Bluetooth-based application is the least intrusive form of mobile tracking and provides the most reliable output to identify the other people that a given individual would have been in contact with recently.

Bluetooth tracking is based on proximity and operates by measuring the "received signal strength indicator" of a connection to estimate distance (i.e., the stronger the signal the closer the devices). GPS tracking, as used in China's COVID-19-related health care application, is considered more intrusive, as it operates by using satellites to actively locate individuals by pinpointing their locations based on proximity to a given area. In addition to privacy concerns, questions have been raised regarding the accuracy of GPS location tracking.

If it is to maintain public trust and transparency, the NHSX will need to consider operational strategies regarding the information gathered by the COVID-19 application in addition to technological aspects of the initiative. The NHSX will need to develop a clear exit strategy, which will allow it to inform users of the envisaged periods that the gathered data will be retained, aligning with the requirements of the General Data Protection Regulation, and set these data retention periods out in a simple and easily digestible manner.

The NHSX needs to consider rules and guidelines for how the data processed in relation to the COVID-19 application will be erased following the pandemic and not kept longer than necessary for any purpose other than those disclosed at the outset. Implementing effective safeguards is likely to be an important factor in fostering trust among the U.K. population and making the rollout of the COVID-19 application a success.

GDPR Feasibility and Cybersecurity Considerations

Because of the volume and sensitive nature of the data likely to be collected by the COVID-19 application, data protection and cybersecurity concerns should be of paramount concern to the U.K. government. The processing of personal data through the COVID-19 application will need to comply with the core data protection principles set out in Article 5 of the GDPR.

The European Commission has advised public health authorities to abide by European Union legal principles (especially the principle of data minimization) when processing personal data for COVID-19-related purposes, calling for a harmonized approach when employing mobile applications to combat the pandemic to ensure that technological tools can interoperate across the EU. The European Data Protection Board has announced that its technology expert subgroup is heading subgroups to produce guidance on key aspects of data processing (including for geolocation and tracing tools) as countries use data processing to fight against COVID-19.

Lawful Processing

The processing of personal data gathered by the COVID-19 application (and more generally any COVID-19-related applications) must be grounded in a legal basis provided for in Article 6 of the GDPR and, where the processing of special categories of data is involved, also with one of the conditions under Article 9 of the GDPR. Special categories of data are sensitive data that are subject to further processing requirements under the GDPR and include genetic data, biometric data and health-related data.

This two-step analysis must be carried out at the outset of a project and prior to the processing of any personal data. The legal grounds under Articles 6 and 9 of the GDPR may be supplemented by specific pieces of legislation at a national or EU level to justify conducting the processing for the purpose of monitoring the spread and minimizing the impact of COVID-19.

The NHSX, as a public body, will most likely rely on Article 6.1(e) of the GDPR, which requires that the processing of personal data be necessary for the performance of a task carried out in the public interest, in the exercise of official authority, or to protect the vital interests of individuals. The NHSX should avoid relying on consent as the lawful basis for processing, as both the GDPR and the DPA 2018 make clear that consent is likely to not be given freely where the controller is a public body.

Core GDPR Requirements

When considering the implementation of the COVID-19 application, the NHSX should contemplate the following core GDPR requirements that would apply to the processing of data:

Risk Analysis: Although certain exceptions may apply to the NHSX as a public body for carrying out data protection impact assessment pursuant to Article 35 of the GDPR, it is advisable and best practice to keep a written record of the risk-based decision-making process associated with the development and implementation of the COVID-19 application.

Transparency: The NHSX will need to provide an external privacy notice made available to the general public upon accessing the COVID-19 application. This notice will include the prior information required under the GDPR and identify, for instance, which types of personal data will be processed, the categories of data recipients, and the purpose(s) sought for such processing.

Security Safeguards: The NHSX should apply strict measures to protect the security and confidentiality of such personal data, which can be done by implementing encryption (in transit and at rest), and, wherever possible, at the least anonymize data or aggregate and anonymize the data processed.

Accountability: The NHSX should keep clear and up-to-date records of actions taken in relation to processing.

International Transfers

To the extent that any data processed by the COVID-19 application would leave the U.K. and be transferred to third countries located outside the European Economic Area, such transfer would most likely be inconsistent with the GDPR unless one of the derogations under Article 49 of the GDPR applies. For security purposes, international transfers made to combat the pandemic in a collaborative global fashion should be undertaken in an aggregated and anonymized manner to the extent possible.

Cybersecurity Considerations

The development of the COVID-19 application presents an opportunity for cybercriminals to exploit the current crisis. Adopting appropriate safeguards — such as (1) encryption, (2) aggregation and anonymization, (3) frequent monitoring of systems, and (4) regular updates against known bugs and vulnerabilities — will be paramount in combating cybersecurity threats and ensuring that sensitive data does not fall prey to criminals.

The NHS already has a cybersecurity model (Cyber Security Support Model) providing for a set of security requirements for NHS organizations to comply with, in line with best practice, which would equally apply to NHSX and the COVID-19 application.

Key Takeaways

The development of COVID-19-related applications has formed part of the exit strategy of several countries seeking to maintain suppression of COVID-19 following the ending, or easing, of lockdowns (or to supplement lockdowns) and appears to be an emerging trend.

Such applications aim to test and trace users, based on health information provided, to confirm whether individuals have tested positive for COVID-19, and if so, notify other users deemed to have been in close proximity with the infected individuals. Depending on how the applications are developed, they can potentially help determine if users should be permitted to enter buildings.

Successful deployment of health monitoring applications on mobile phones as a suppression method has the clear potential to mitigate damage to the economy caused by the pandemic. A key challenge facing the developers of such mobile applications will be garnering high enough levels of adoption, with Oxford researchers postulating that at least 60% of the target population will need to opt in to using these applications for them to be effective.

At the heart of such mobile applications and the COVID-19 application lies data protection and cybersecurity concerns. Even during a pandemic, data protection laws continue to apply and should be followed when processing personal data in the context of COVID-19-related applications; this should help maintain public trust, which in turn will support the success of these suppression techniques by promoting high levels of user adoption.

The U.K. will need to carry out a balancing exercise, as although positive domestic laws could allow personal data necessary to contain the virus to be processed for the purpose of monitoring the spread and minimizing the impact of COVID-19, this must be done in a manner that ensures there are safeguards in place to protect the individuals whose data is being processed and their civil liberties.

As public health experts in the United States formulate recovery strategy, they will no doubt watch the U.K. experience closely. The role of serology immunity testing and technology — alone and in tandem — are much in play, as is an exit strategy that involves tracking, aggregating and reviewing personal electronic health data.

Whether Americans would ever have an appetite (much less tolerance) for such a solution is a great unknown. Whether American policymakers would ever ask may depend on whether it first works abroad.

Correction: An earlier version of this article misstated the dates on which the FDA released and updated guidance on the commercialization of serology immunity tests. The errors have been corrected.

Scott C. Hopkins and William (Bill) McConagha are partners at Skadden Arps Slate Meagher & Flom LLP.

The authors wish to thank Skadden counsel Eve-Christie Vermynck, associate Pamela I. Amaechi and trainee solicitor Sagar Singh for their contributions to this article.

[1] See Skadden's client alert, "COVID-19, Contact Tracing and Data Protection in the Workplace."