COVID-19: operators need to overcome privacy issues in order to help combat the coronavirus threat

March 2020

Justin van der Lande

Operators are already proving their worth to societies around the world during the COVID-19 crisis by enabling home working, providing entertainment and supporting self-isolation, but there is more to be done. For example, mobile operators in some countries are providing proximity checking. This is where mobile phone data is used to warn subscribers that they may be infected as a result of being near an infected person. These insights can be used by government health departments or government-backed schemes to help citizens and limit the spread of the coronavirus.

Mobile network providers can pinpoint a subscriber's location through the triangulation of wireless RAN data, any IP addresses used or a device's GPS signal. Singapore's TracTogether app uses Bluetooth to gain more-accurate location data, and to measure the proximity to other phone users. Location data can be used to create a timeline for each infected person in order to retrace where they have been during the time in which they have been infected (approximately 5 days). This can then be linked to the location data of other users to identify all of the subscribers that have been in the proximity of an infected person. Depending on the precision of the location data, this can be accurate to a few square metres. For example, TracTogether identifies all users that have been within Bluetooth range. Other factors can also be considered, such as the number of phones in a known venue or location (for example, a train carriage or bus), and the time spent in each location by the infected person; this can help data analysts to model the probably of an infection having taken place.

There are several barriers to tracking an infected person's location

Tracking an infected person's location and determining the number of other people that have been in their proximity is not without its challenges.

- Personal data privacy laws prevent mobile phone companies from using data without permission.
- Tracking every mobile customer's location and then comparing this data to the known journey of an infected person requires a huge amount of computational power.
- Any single operator does not have access to the data from all mobile subscribers; this data would need to be shared between all mobile network providers within each country. Initiatives such as Weve in the UK have attempted to achieve this in the past.
- The speed at which data can be analysed, insights created and alerts sent to each subscriber is critical in being able to reduce the number of infected people. However, it is likely that the time scale for this will be in the order of days, by which point further infections may have occurred.
- Operators may not want to be involved in such an initiative due to the potential for negative publicity.
- It may already be too late to execute a 'containment' strategy in many countries.

- Google and other technology companies such as Facebook and Fitbit also have access to customer data that could do the same function, meaning that operators do not necessarily need to be involved.

The rate and reoccurrence of COVID-19 infections could be reduced if the above challenges can be addressed.

Key concerns over data privacy regulations can be overcome

- Operators may gain consent from users of downloaded apps (countries including Singapore, Israel and South Korea have adopted this approach).

- Governments could enforce a specific clause in article 9 of the GDPR that allows for the processing of personal data without consent if it is needed to protect cross-border threats to health.

It may be quicker and easier to use an app rather than waiting for a more-libertarian government to test out data privacy laws. The use of an app also means that citizens are left in control, which is likely to be advantageous in gaining citizens' co-operation. Perhaps more significantly, the computational effort required to use network data to discover and trace each subscriber's journey for the past 5+ days and analyse how these journeys intersect is extremely large and expensive, whereas an app-based approach is simpler, potentially more accurate and requires much fewer computational resources.

Concerns over data privacy are real, but the population is unlikely to have major concerns given the situation

Tracking infected citizens is not the only potential use of location data. Subscribers can also be tracked to provide governments with a detailed picture of their travel patterns in order to understand what regulations may be needed and how effective they would be once implemented. For example, the data could be used to see how strongly 'stay at home' advice is being adhered to by citizens.

Different strategies to social distancing have been adopted but being able to reach each citizen directly with trusted advice is required in all cases. Location data could enable this to go beyond general advice (illustrated in Figure 1), and personalised messages could be sent from the government if a citizen is seen to be ignoring a request to stay at home, for example.

Figure 1: Direct government messaging in the UK during the COVID-19 outbreak

Source: HM Government via Vodafone UK, 2020

Containment of the virus is not possible in most affected countries or states, but the reduction in the number of reoccurring infections is just as significant in preventing a fresh outbreak. This must be closely monitored until all virus cases have been resolved or until an effective cure has been developed. The ability to return to a containment-based approach will therefore become a more-significant strategy as the overall number of COVID-19 cases reduces and normal life returns.