On the proportionality of Aarogya Setu

Subhashis Banerjee* Bhaskaran Raman† Subodh V. Sharma*

May 19, 2020

[Updated on July 7, 2020]

The excessive push for Aarogya Setu by the government as the major instrument in our fight against Covid has been extraordinary. While several commentators have raised serious concerns about the privacy and trust issues related to the app based approach, a careful analysis of its proportionality also requires a scrutiny of its effectiveness and utility. This is especially important because no detailed and credible evaluation of its efficacy is as yet publicly available.

According to virologists Covid-19 can transmit in two ways - by direct person-to-person transmission by inhalation of droplets or aerosols carrying the virus, or by inadvertently picking up droplets from contaminated surfaces. For the former the exact dependence of infection risk on proximity is as yet unmodelled, but it is believed that the person-to-person distance should approximately be within $2m$ for sufficient virus load inhalation. For the latter, the virus can survive on some surfaces, particularly on hard metallic ones, for several hours or even days.

Electronic risk assessment uses two main principles - GPS based geolocation and Bluetooth based proximity sensing.

GPS is often unavailable indoors. Even outdoors, 30-40% unavailability in dense metropolitan areas like Mumbai is common. And even when GPS is available, it can have errors of several tens of metres on a consistent basis. Thus GPS is clearly not reliable for risk assessment for within $2m$ person-to-person direct transmissions, especially in dense gatherings. Declaring everybody within a few meters of an infected individual at potential risk will generate too many false positives. Moreover, mere colocation does not necessarily imply high risk for a cautious and aware person, and the risk may be overestimated. GPS is also unreliable for indirect transmissions. The proximity with an offending indoor surface is likely to be missed altogether resulting in false negatives.

For Bluetooth based proximity sensing each device transmits low energy radio beacons isotropically in all directions at periodic intervals. A listening device picks up the signal and that establishes a communication channel between the two devices. Distance is usually estimated based on the strength of the received signal.

First, it is unclear what interval rate of radio transmission is adequate for effective risk assessment of direct person-to-person infections. Too frequent transmissions will drain out batteries and too wide gaps in time will lead to false negatives.

Second, it can also generate too many false positives, for example by overestimation of risk across large distances in open spaces, across walls - which radio can penetrate but the virus cannot - and across floors. False negatives are also possible because of weakening of radio signals through human bodies, for example if the victim carries the phone in her front pocket and an infected person stands close behind her in a queue.

Third, for indirect transmission of infection, since the virus can survive on contaminated surfaces for hours or even days, the intersection of smartphone trajectories will need to be computed not only in space

*Computer Science and Engineering (also associated with the School of Public Policy), IIT Delhi
†Computer Science and Engineering, IIT Bombay

but also over large temporal windows. For this, Bluetooth based proximity sensing - which are isolated communication events over narrow temporal windows between two smartphones - will be ineffective.

It is a basic principle of engineering that all measurements must come with an associated error model clearly specifying the least count and a confidence interval for the measurement. For risk measurement this requires precise estimates of the rates of false positives and false negatives. Aarogya Setu does not specify such rates. Moreover, the principles by which such rates can be estimated are also not clear, either for GPS or Bluetooth proximity based estimation of infection risks.

There seems to be a leap of faith from GPS colocation and Bluetooth radio proximity to estimating a risk score for infection transmission. This is compounded by the low penetration of smartphones in India. Too many false positives and false negatives may lead to an unbounded noise-to-signal ratio for infection transmission. Such high noise may actually create confusion and detract from the main effort by sending administrators and policy-makers on wild goose chase. It seems entirely unlikely that such apps can do anything for estimating risk of infection at the micro-level that local community based manual contact tracing cannot do much more effectively. We have the examples of Kerala and Dharavi in Mumbai where such manual methods have led to impressive containments. At best, GPS based geo-location can enable identifying hotspots at the macro-level. Moreover, the utility of contact tracing is limited when there is community transmission, as many instances of spreading will not be caught by it.

The privacy aspects of Aarogya Setu have also not been well thought out. Unlike most other contact tracing applications - for example Apple and Google's proposal, DP3T, MIT's Private-Kit and PACT, Singapore's TraceTogether etc. - it appears that Aarogya Setu uses a static transmission id for every smartphone, fixed at the time of registration. The other applications mentioned above generate a new random token to be used as a fresh id after a pre-specified interval. Aarogya Setu also collects more metadata compared to the other apps - for example the timestamp of the contact, the MAC address, the Bluetooth model name and number of the contacted device. Moreover, the other applications - except Singapore's TraceTogether - assume the centralised server to be untrusted. In contrast, the centralised server is assumed to be completely trusted in Aarogya Setu.

The static id and the additional metadata that Aarogya Setu collects - especially the time stamps and geolocations - make it vulnerable to privacy attacks by users. By collecting auxiliary information from secondary sources, and by possibly colluding with other users, an attacker may orchestrate a triangulation attack to deanonymise and identify a person deemed to be at high risk of spreading the infection.

Also, Aarogya Setu reveals an estimation of "infection risk" within a radius of $10 - 500m$ to its users. This seems unwise when the stigma and fear have grown larger than the disease, and there are several reports of doctors, service staff, as well as members of vulnerable communities being targeted and stigmatised for fear of spreading the virus.

Though the source code of a version of the app is now public, the design details outlining the conceptual principles, and the server-side details, are not publicly available. Without any clearly specified *access control protocol* and *purpose limitation architecture* at the central server, and in the absence of any *regulatory oversight*, illegal identification of users and other violations are also possible at the server. Public applications definitely need to be more transparent in their design.

Aarogya Setu appears to be a classic example of technological-solutionism. Coupled with inadequate privacy protection, it does not appear to be proportionate. We need to introspect about the processes that led to its emergence as a foremost scientific and policy response tool in our fight against Covid.