Apps for COVID: to do or not to do

Subhashis Banerjee[*] Bhaskaran Raman[†] Subodh V. Sharma[*]

April 14, 2020

The COVID virus crisis has brought out some much required public spiritedness in the Indian science and technology community, and there is now a strong urge to contribute meaningfully. A popular response among technologists has been to develop surveillance apps on smartphones, for contact tracing to keep tab on the disease spread, for geofencing to enforce quarantine, and for gathering data for modelling the spread of the contagion. Indeed, there are several reports of efforts and successes of such endeavours from all over (Krishnan, Servick, Strickland, Hamilton, Heaven), and several commentators have alluded to the possibility of pervasive under-the-skin surveillance in a post-COVID world (Harari, Mehta, Macaulay).

There has also been a spurt of indigenous efforts to build such apps (Singh, Johnson, Money Control News, Sengupta, ET Online), and there is unbridled enthusiasm among our students of technology to pitch in. It is indeed true that contact tracing is crucial for effective combating of the spread of the contagion, but can it be done accurately and reliably with such hurriedly engineered apps? Some caution perhaps is in order, especially related to the risks and reliability.

The implicit sentiment in developing and deploying such technology is that privacy concerns should take a backseat in this health emergency. This has two dangers. The first is that the invasive technology could continue well beyond the health emergency. The second, and perhaps more important, is that violation of privacy is *especially* a problem in the context of a health crisis where fear of the virus and the associated stigma spreads much faster than the virus itself.

The apps are not risk free, especially in India

Privileging utility over privacy for such crucial applications is indeed typical, but the balancing requires careful examination (Pratap), especially when the details and whereabouts of corona-affected people are revealed to authorities and public.

The authorities in India are not known for their discretion, and there have been instances where they have leaked information about quarantined people through WhatsApp (Vatyam). In a society prone to prejudice, discrimination and attaching stigma to ailments, the cost of false positives can be significant. Indeed, there are reports abound about ostracising airline staff (Vaid), denying houses on rent to doctors and other health workers or asking them to leave (Sharma), and refusing service to people from the northeast (Rakesh), on the basis of mere suspicion that they may be carriers of the contagion. Denial of services and facilities to persons flagged by such apps, and persecution, especially if they belong to marginalised communities, are real possibilities.

Technology deployment always has to be society and culture specific. Some solutions developed in the west are reported to have features for informing others of the locations of COVID-positive individuals (Khanna). Such features have also found their way into apps planned by Indian groups

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

[†] Computer Science and Engineering, IIT Bombay

(Express Computer, ET Online). Public dissemination of such information can be hugely counterproductive in our society where there is stigma associated with the virus. With self-declared social vigilantes taking law into their own hands, such information can be downright dangerous.

And, in the absence of any data protection standards, there is always the possibility that the collected data along with location traces may be used for other purposes after the current threat of the virus is over. Such unchecked uses, over which individuals who participated in the data collection process may have no control, may pose serious threats to privacy and civil liberty.

Moreover, errors in data collection, whether in the estimate of the number of infected persons within a space or time limit, or high rates of false positives or negatives in estimates of the transmission of infection, will inevitably result in unreliable contact tracing and modelling of the disease spread. Network and compartmental models of epidemiology are parametric, and errors in parameter estimation can result in inaccurate and misleading models. Unstructured collection of data with imprecise understanding of future use and unmodelled errors can make the data untrustworthy for any serious epidemiological application.

Reliability is an issue

It appears that the COVID infection spreads either by direct inhalation of droplets carrying the virus, or by inadvertently picking it up from contaminated surfaces. In the former case the victim needs to be in proximity of an infected person. Hence, avoiding false positives requires contact tracing at a resolution higher than what is offered by GPS or Google maps, especially in dense gatherings, and neither of them can work indoors. Geolocation from cellular data offers even lower resolution, and, for mobiles to interact with each other to record proximity - for example with Bluetooth (ET Online) - the app use must be universal. Also, since the virus can survive on contaminated surfaces for several hours, the intersection of smartphone trajectories will need to be computed not only in space but also over large temporal windows. For this, proximity sensing will be ineffective. Proximity sensing using Bluetooth can also generate too many false positives, for example across large distances in open spaces, across walls or across floors.

In either case it will require data aggregation from multiple smartphones to compute intersections of trajectories. Such aggregation will be hard to implement decentralised at scale, and centralisation will require additional infrastructure. Even with centralised aggregation, rigorously estimating the dynamic network parameters and the associated error models will be a non-trivial task, especially without near universal participation. Modelling disease spread accurately at the micro-level with data collected through such apps appears to be a research problem that offers considerable challenges. It is entirely unlikely that any reliable model can be rigged up in a hurry, even for contact tracing. At best, mobility data (Fitzpatrick) may be used for modelling macro-level patterns of infection spread, that too with several simplifying assumptions with uncertain error models.

Besides, making such apps universal, and centralised aggregation with support from mobile service providers, Google and indoor WiFi providers, will certainly be beyond individual app developers and will require governmental support. China did a lot of it with face recognition technology, with a very high density of camera deployment, and the infrastructure was already in place (Krishnan). It is unlikely that such complex surveillance can be implemented in a hurry, in the middle of a pandemic spread. And, for such large scale centralised surveillance there are serious privacy and data protection concerns that need to be addressed - in terms of legitimacy and proportionality, regulatory oversight, access control and purpose limitation (Pratap, Banerjee and Sharma).

On the whole it may be unproductive to develop such systems without expert epidemiological and disease control advice. The risks of false positives are too many. Deploying a large number of unreliable systems may divert useful resources and actually detract from the main effort.

Geofencing of smartphones will certainly be easier to develop (Money Control News). However, the efficacy for enforcing quarantine is doubtful with simplistic solutions, both because majority do not have smartphones and because smartphones can be switched off and solutions like 'take a selfie at prescribed times' are too easy to bypass. Moreover, the continued presence of a smartphone within a quarantine zone does not necessarily imply the quarantine compliance of the owner. Breaking some of the defence mechanisms may be possible, and protections against breaking them are also possible. One needs to think through all this and desist from hurried app rollouts.

There can be simpler solutions

In the context of contact tracing, a simple app in which users can voluntarily switch on recording of Bluetooth-based contact trace, and perhaps manual entry and geolocation too, may be useful. The app can also locally maintain a list of contacts they meet, anonimized as random tokens, such as in the approaches taken by TraceTogether (Government Singapore, Canetti et al.). The user may then *voluntarily* choose to inform people in the contact list in case she tests positive, and may even voluntarily disclose the location tracks (Heaven). While the reliability may still be low, but so may be the risks.

The usefulness of contact tracing is maximized if a large number of people install the app. This can in turn happen only if users *trust* the system. If users fear that they may be victimized due to information sharing by the app, they are unlikely to install the app in the first place. This stresses the importance of aspects like *anonymity* and *voluntary disclosures* in any contact tracing system. Most importantly, the operational and design details of all such apps (ET Online) must be made public.

While one must be cautious in the use of technology for any purpose, in the current situation there are indeed various other technology needs which do not involve tracking and tracing people at large (ISRC). Some examples include remote patient advice by doctors for non-emergency situations, appointment systems, queue management to avoid crowding at hospitals or the local grocers, management of ration distribution and home delivery of ration for those who need it etc. However, all such apps need to be developed, if at all, in consultation with people working on the ground.

Avoid techno-determinism

On the whole, self-compliance through education and sensitization may be a more productive approach than enforcement. Working towards building community resources and community empowerment may turn out to be more fruitful than building apps. A fetish for technological fixes for everything may actually come in the way of looking for simpler solutions. It may also preclude developing a comprehensive understanding of the complex problem involving dimensions in biology, modelling and data analysis, epidemiology, sociology, economics, politics, and, above all, human compassion.

Acknowledgement: We thank Manoj M. Prabhakaran for bringing us together, and for several useful suggestions and pointers.