AROGYA SETU APP: UNDERSTANDING THE PURPOSE AND ISSUES

*- Samarth Garg**

Abstract:

The entire world is at a standstill due to the pandemic i.e. novel coronavirus, it has affected lives as well as all types of livelihood. The virus which started to spread in the Wuhan region of china is now present all over the globe. The outspread has proven to be incessant and fatal. As of now there is no cure available for the pandemic, the researchers and doctors all around the world are working to find a vaccine or antidote which could curb the pandemic. The only available treatment is lockdown and social distancing.

The key to fight this virus is testing as many people as possible but considering India's dense population it is really difficult for the authorities to individually check all the citizens of the country so to overcome this the country has undertaken contact tracing. Not only India but many countries around the world are using this technique to detect covid-19 positive patients. India has developed an app called Arogya Setu which has proven to be helpful during these trying times but hackers and cyber law experts are raising issues regarding the apps violation of privacy and many more.

The article aims to understand the usage of the said application and what are issues raised about the application and its vulnerability.

Introduction

The Narendra Modi government propelled the Aarogya Setu mobile application on April 2. It is Indian COVID-19 tracking application. It is created by the National Informatics Center which goes under the Ministry of Electronics and Information Technology. To spread attention to COVID-19. To spread awareness of COVID-19. To link fundamental coronavirus related health information and services to the citizens of India.

It utilizes the cell phone's GPS and Bluetooth highlights to track the coronavirus infection. With Bluetooth, it determines the hazard if one has been near (inside six feet of) a COVID-19 contaminated individual, by looking over a database of known cases across India. Utilizing area data, one can decide if a specific area is one of the contaminated territories. It is a renewed rendition of a previously developed application called Corona Kavach. The motivation behind this created application was to embrace the procedure of contact tracing.

Understanding Contact Tracing

As per the WHO, contact tracing happens in three stages to be specific (a) contact ID; (b) contact posting; and (c) contact development. Specifically, contact tracing is a pillar which helps public authorities in containing and the pace of transmission of the infection. This pace of transmission is estimated by the unit R0 (R nothing) which basically hints at the number of individuals a tainted individual can spread the ailment onto.

Contact tracing has customarily been managed using on ground work force and volunteer armed forces. In any case, with the universality of cell phones, which gather huge troves of individual data, governments over the world accept reconnaissance can help with quick contact tracing. In any case, attributable to the eccentricities of the coronavirus, specialists over the world are starting to understand the constrained adequacy related to area observation (both with cell tower information and with GPS signals).

Subsequently governments and different gatherings have either discharged or are creating cell phone applications that utilize Bluetooth guides or GPS signals to log examples wherein a user's gadget interacts with other users' gadget. As the user of the application is tested COVID positive, because of the feature of contact tracing it authorises the administrators of the application to spot their close contacts who came in close proximity with them in the prior days or weeks to break the chain before it spreads incessantly.

Purpose of developing the application

1.To spread mindfulness among Indian residents about the Novel Coronavirus. It is planned for increasing endeavours to proactively educate residents about warnings and best works on relating to containing the spread of infection. To build up joins between the legislature and individuals to educate them about health service.

2.People and specialists will remain informed in the event that they have run into somebody who has tested positive for coronavirus.

3.It works on Bluetooth-based innovation. Absence of a web network will not be a hindrance.

4.The application suggests a few estimates, for example, Self-Assessment Test, Social separating, do's and don’ts. It illuminates the careful steps.

5.According to the announcement by the Prime Minister's Office, it could likewise be utilized as an e-pass for travelling.

5.On the off chance that a user is at high hazard, the application will prompt him/her to go for a test at a close by testing focus and call the toll-free number 1075 right away. The helpline number for each state is additionally accessible.

Issues concerning legitimacy

Identifying with the application a lot of issues have been brought up whether it is penetrating the crucial right to protection. Lawyers and information security specialists have raised worries over the legitimacy of these rules as this Disaster Management Act doesn't contain any arrangement or method with respect to the assortment of individual information of the residents thus far as the position to make it obligatory for download is worried, there is no administrative or lawful back that exists for the application.

In spite of the fact that this move is by all accounts the need of great importance, it brings some genuine worries up in this period of information assurance, particularly compared to the fundamental right to privacy under Article 21 of the Constitution of India[1]. The point of reference

* *Samarth Garg is a student at Maharashtra National Law University, Mumbai.*

built up with the Aadhar judgment was applied again when the administration made it obligatory to download the application, particularly in situations where one chooses to travel either via air or railroads. After the loosened-up talk on the Aadhar Act, an approach, for example, this one certainly can possibly lift the inner mind fears we as a whole have with respect to our protection

1.With the making of such frameworks, come new dangers of institutionalisation of mass surveillance Fundamentally, India comes up short on a thorough information law, obsolete observation and interception laws, or any significant recommendations for important change. In areas like calamity alleviation, most applications which are indicated as 'contact following' advances, they regularly decay into frameworks of development control and lockdown implementation. frameworks like this wrongly encourage individuals to pre-emptively step through exams then there is a hazard that general wellbeing frameworks might be overpowered rashly. It might likewise intensify the dangers related with the reaping of individual information like persoanl data, and furthermore observe the formation of new protection intrusive frameworks.

2.Aarogya Setu" isn't not an open-ended source- The Aarogya Setu source code is not an open source code. By making the code accessible increases transparency and this also helps in improving security of the application as the source code is there for network review. The application fundamentally gathers individual information from client mobile phones and PDAs are a massive vault of individual information of clients and of a client's contacts and colleagues. In this situation, keeping the source code of such an application restrictive isn't fitting.

3.Personal Data Collected and its Use – The application, according to its security strategy gathers the accompanying individual data during enrollment and stores it in the cloud: (I) name; (ii) telephone number; (iii) age; (iv) sex; (v) calling; (vi) nations visited over the most recent 30 days; and (vii) regardless of whether you are a smoker and an individual's present ailment gathered through a progression of inquiries when the application is run just because to assess the state of the client. In addition, the App ceaselessly gathers the area information of the enlisted client and keeps up a record of the spots where the client had interacted with other enrolled clients.

[1] THE CONSTITUTION OF INDIA. (n.d.). Retrieved June 17, 2020, from https://www.india.gov.in/sites/upload_files/npi/files/coi_part_full.pdf

Proviso 2 (an) of the Privacy Policy states, concerning the utilization of gathered information, that:

a. The personal information collected from under Clause 1(a) above, will be kept locally in the Application on your gadget and will only be uploaded for utilisation by the Government of India (i) in anonymous, datasets for the only reason for creating reports, heat maps and other statistical visualisati**ons.**

b. Any personal information uploaded to the cloud will only be used for the purpose of informing you, or those you have come in contact with, of possible infection. Such personal data may also be shared with other necessary and relevant people as required in order to carry out necessary medical and administrative interventions and research[2].

This proviso empowers the Government to share individual data transferred to the cloud with "such other vital and pertinent people" so as to "complete fundamental medical and regulatory intercessions.This is problematic as the clause is broadly worded allowing the data to be shared with anyone that the Government feels like sharing.

4. "Limited Liability" - The liability limitation clause of the Terms of Service restricts the Government's obligation regardless of whether off base data is given by the App or if there should be an occurrence of inability to produce genuine positives. It is relevant to take note of this vindicates the Government's risk in the event of any mischief caused because of erroneous data. In this manner, the App's approaches render the App as only another information getting exercise.

Besides, the risk condition additionally excludes the Government from obligation in case of "any unapproved access to the user's data or alteration thereof" (accentuation provided). This implies there is no risk for the Government regardless of whether the individual data of app users are leaked.

5.Restrictions on reverse engineering. Reverse engineering is a procedure through which individuals are able to understand a computer programme and study how the programme operates and if the programme is doing only for what it was developed.

[2] Our Concerns With The Aarogya Setu App. (n.d.). Retrieved June 19, 2020, from https://sflc.in/our-concerns-aarogya-setu-app

It is essential for security researchers to study and analyse the operation of an app like Aarogya Setu which is potentially a surveillance instrument that collects the movements and geolocation data of its users.

A clause in a Terms of Service cannot take away a statutory right provided by a Central Act. The former infringes the latter right provided by the constituion. Therefore, this provision within the Terms of Service must be erased.

The Aadhar Act, 2016[3] was passed with the respectable aim of unifying authoritative identification in India by providing a unique 12-digit code on a biometric basis to every citizen. However, there was a serious turn of events as the Aadhar linking base widened its scope from ration cards to bank accounts and eventually worked its way into our mobile phones. The expression "you needn't be apprehensive on the off chance that you don't have anything to stow away" turned into an informal saying of the law.

Before any move was made, the law experienced genuine lawful inconsistencies, for example, Section 57 which took into account private partnerships to get to Aadhar information so as to validate a client. Besides, Section 33(2) of the demonstration considered revelation of a personality holder's private data in the quest for national intrigue, while the term 'national intrigue' was not characterized under the Act. Both these arrangements were struck somewhere around the Supreme Court of India, and a few different changes to the law were requested to handle any encroachment of security.

Also, the Aarogya Setu application was made an obligatory component for all private and public representatives during the lockdown as a way to find the individuals who might be affected and the individuals who might be in closeness to the corona positive. One of the principle debates behind the privacy policy of the Aarogya Setu is that its source code is that it is not open to the general population rather than other contact tracing applications being used by outside countries, for example, the U.K., Singapore, Israel and Australia. Because of this worry, I.T. secretary Ajay Prakash Sahwney said that he would not open his source code to general society as it would raise more issues to be managed, which is something the legislature can't bear to have right now.

[3] Key Highlights of the Aadhaar Judgment. (n.d.). Retrieved June 17, 2020, from https://sflc.in/key-highlights-aadhaar-judgment

Technical issues

At the absolute starting point of the application's launch, several legal and technological specialists distinguished strategic issues with it, for example, its Application Programming Interface (API) which would permit different applications, sites and administrations to get to the information stored in the Aarogya Setu application. This could lead to exposure of sensitive data, for example, the user's mobile number to online administrations without the assent of the client.

Additionally, the application depends on self-evaluation including through which the user would have the option to provide details regarding their side effects and contribute all the while. In any case, this methodology appears to be amazingly counter-gainful as various individuals conveying the infection were seen as asymptomatic. This would likewise expand the number of bogus positives and bogus negatives which would prompt more complexities.

Lastly usage of bluetooth and GPS system increases the chance of getting the location of the user all the more risking the chance of revealing the identity.

These deficiencies combined with the legitimate issues confronting the application guarantee that while Aarogya Setu may not be viewed as a failed operation, it can't be pronounced to be an effective one either. The application may have had the option to accomplish its targets yet it was being used at the expense of user's entitlement to right to privacy

How did government react to raising issues?

The Central Government has, in light of the security concerns, provided with a lot of rules on 1st may for handling the information obtained through the application that confines the storage of data up to a time of a half year. Simultaneously, it permits the users to look for the cancellation of their records inside 30 days of mentioning the same and punishes violators of specific rules with a prison term. These rules were actualized to guarantee the safe administration of the information gathered by permitting the assortment of limited data.

According to the government's mandates, this data must be imparted to educational establishments with the end goal of exploration. This would be done by expelling any personal data which may prompt the identification of the user of this application. Any infringement of these rules would make the miscreants be punished laid under Sections 51 to 60 of the Disaster Management Act, alongside whatever other lawful arrangements that might be appropriate.

1. Reverse Engineering no longer penalised, source code yet to be made open: Clause 3 of the past terms of administration denied reverse engineering of the App. This has been done away in the refreshed terms of administration implying that any individual who figures out the App won't be punished any longer. It is an inviting step notwithstanding, the source code of the App is yet to be made open source.

2. Functionality reached out past contact following, a building block for India's health stack- This could be another way of looking at the aap, not only it aims to protect the people during the pandemic but it could help in augmenting the health infrastructure.

The government might be held subject if there arises an occurrence of unauthorised access to the past terms of administration exculpating the legislature of any obligation at all. Condition 6 of refreshed terms of administration expresses that "the Government of India will put forth best attempts to guarantee that the App and the Services proceed as portrayed yet won't be held liable for (a) the failure of the App or the Services to precisely recognize people in your vicinity who have tested positive for COVID-19; (b) the exactness of the data given by the App or the Services concerning whether the people who have interacted with people been contaminated by COVID-19.

This implies now the Government might be held obligated if there is an occurrence of unapproved access to the user's data or any adjustment to it or some other risk emerging from data breach and so on.

3. No option to request deletion of demographic data: Clause 5(e) of the Protocol permits the user to demand cancellation of its demographic information. No such option is visible for the refreshed privacy policy or terms of administration. Neither do terms of usage determine if un-installation of App will add up to erasure of demographic information

The App has neglected to provide deletion of whole reaction information, for example, demographic information, contact information, self-assessment information and area information. Allowing a user to erase its segment information only serves little or no purpose.

4.No harmonization between the Protocol and the App: While the Protocol expresses that the reaction information of a user will be for all time erased in 180 days from the date on which it was gathered, the renewed Privacy Policy despite everything states that information of a COVID-19 patient will be held till 60 days after such individual has been proclaimed free of COVID-19. It is as yet indistinct if the information of a user will be held for the span indicated in the Protocol or in the Privacy Policy.

Contact tracing Apps: A comparative analysis

Trace Together application of Singapore; and second is the Private Kit application of Massachusetts Institute of Technology (MIT) are the two models contrasted with India's Aarogya Setu. Trace Together application doesn't gather area information and just expects access to the client's Bluetooth. This information gathered by the application is anonymised, and the clients have authority over their own data. Likewise, the application's strategy plainly specifies that the information will be utilized uniquely by the Ministry of Health of Singapore. Further, Private Kit application permits clients to impart their location to health specialists. The application's main role is to contact trace however the information can be utilized for examining individuals' prosperity, network traffic examination and asylum relocation. Along these lines, a few elements of this application probably won't be in accordance with the purpose limitation principle. The Aarogya Setu application expects access to GPS and Bluetooth of the user, which is more than what is required by Trace Together and Private Kit for contact following. As referenced over, the application's self-recognizable proof test requires a client's delicate data, which is far more than the data gathered by both the models. The application's arrangement doesn't make reference to any techniques to keep the information anonymised, and there is no notice of a particular service approaching this information. This obscurity is inordinate when contrasted with the other two models, and accordingly, the Aarogya Setu application runs conflictingly with standards of direction impediment and information minimisation.

Conclusion

Aarogya Setu has been considered as one of the key instruments for the administration in the fight against the COVID-19 pandemic. Contact tracing has been viable in different nations like

Singapore, Japan and many more. But the privacy concerns raised are equally important as the issue brings forth a question of proportionality. This is something similar which happened during the usage of Aadhaar. These things make us realise the importance of the right to privacy. The issues being raised as of now are the transparency and liability issues which are raising serious concerns for the IT community as well as the citizens of the country. For instance, there is a need that the data collected must be processed for a specific purpose, and it must be known to the people. Besides, the administration must legitimize the utilization of the two GPS and Bluetooth for contact tracing in a system that doesn't infringes individuals' privacy. The consolation given by the administration's new arrangement of rules may correct the issue somewhat, yet it absolutely doesn't represent all the lawful defects that confronted the Aarogya Setu application. An unconstitutional practice was executed by the Central Government and it was only taken care of after being questioned by the public on a large scale but it was really important to understand that it was need of the hour and after such questions were raised the government did not fall back rather they came up with cleared guidelines which could ensure that government is not only concerned about the coronavirus but fundamental right to privacy too. The only way forward is bringing the said app under the ambit of the well drafted right to privacy bill which is already in consideration in India, also this step can be considered a stepping stone towards building a better health infrastructure.