An International Registered & Refereed Monthly Research Journal

Studies in Indian Place Names

UGC Approved Journal

UGC Care Journal

**Multidisciplinary Refereed/Peer Reviewed Journal
UGC CARE Listed**

Journal Details

Journal Title (in English Language)	Studies in Indian Place Names
Publication Language	English
Publisher	The Place Names Society of India
ISSN	2394-3114
E-ISSN	NA
Discipline	Social Science
Subject	Social Sciences (all)
Focus Subject	Geography, Planning and Development

Studies in Indian Place Names

AAROGYA SETU APP – POLICY ANALYSIS & FUTURE OF CONTACT TRACING IN INDIA

Md. Mudassir Siddiqui
Ph.D Scholar, Jharkhand Rai University, Ranchi

ABSTRACT

On 2 April 2020, India launched Aarogya Setu Mobile App to help increase efforts to reduce the spread of COVID19, with the aim of enabling Bluetooth-based contact tracing, mapping of likely hotspots and dissemination of relevant information on COVID19. The App has more than 114 million users as of 26 May.2020, more than any other Contact Tracing App in the world. The App is available in 12 languages as well as on Android, iOS and KaiOS platforms.

In order to break the chain of infection, it is important to provide medical assistance and advice to people who may be at risk, especially asymptomatic people, i.e. people who may have contracted the infection that have not yet shown symptoms. Through the app when we take the self-assessment test, by correlating the symptoms that we report along with our location information, the Government of India will have the ability to identify hotspots where disease may be spreading , early enough, so that necessary interventions can be done to control and mitigate the spread of COVID-19.

The Government made it mandatory for all public and private sector office employees to download the Aarogya Setu app. Apart from this, all citizens living in an identified COVID-19 containment zone are also required to have the Aarogya Setu app installed on their Smartphone. The government directive also stated that it will be the responsibility of the heads of the respective organisations, in both private and public offices, to ensure 100 percent coverage of the Aarogya Setu app among employees. So it is very clear that in the process of curbing Covid-19 pandemic in India with the help of technology Aarogya Setu mobile was created.

The very nature of the app was to physically track each individual user, their movement and location but came in contradiction with IT Acts and overtook the Right to Privacy. Any app that tracks who you have been in contact with and your specific location with pin point accuracy at all times is a clear violation of our privacy rights. The somewhat vague and lose nature of the protocol is also a concern. Considering India's horrible past with protecting privacy of its people the inefficient IT Act and the still hypothetical privacy bill didn't provide much hope. One of the main concerns is sharing of this private data with third-party entities.

The App helped identify about 500,000 Bluetooth contacts and helped 900,000 users with advices for Quarantine, caution or testing. Among those recommended for COVID19 testing, it was found that almost 24 percent of them were found to be positive for COVID-19. Comparing this to the average positive result of COVID-19 we find that a total of 145380 COVID-19 positive were found from a total of 3126119 experiments carried out by 26 May 2020. The contact tracing did help but for this our privacy rights were compromised under Disaster Management Act 2005.

Later on after 55 days of launching the app, the open source conversion of the Aarogya Setu App became one of the most required decisions taken by the Government of India. This made the contact tracing process of the app transparent and helped to rebuild and restore the trust of common individual into the constitutional machinery that has been put in place to safeguard his/her interests and rights. Moreover the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 also specified that the app collected data will at most be used for six months. We hope that next time whenever we install or select any government driven application, there is no dark areas in its policy and implementation and we do it with trust and confidence.

Keywords: Aarogya Setu App, Contact Tracing in India, Data Privacy, Privacy Laws, Covid-19 solution

1. INTRODUCTION

On 2 April 2020, India launched Aarogya Setu Mobile App to help increase efforts to reduce the spread of COVID19, with the aim of enabling Bluetooth-based contact tracing, mapping of likely hotspots and

dissemination of relevant information on COVID19. The App has more than 114 million users as of 26 May.2020, more than any other Contact Tracing App in the world. The App is available in 12 languages as well as on Android, iOS and KaiOS platforms. Citizens across the country use Aarogya Setu to protect themselves, their loved ones, and the nation. Many youngsters call Aarogya Setu their bodyguard.

What is Aarogya Setu?

Aarogya Setu is a digital service, primarily a mobile application, developed by the Government of India and intended to protect citizens during COVID-19. It is designed to facilitate the initiatives of the Government of India by informing the people of their potential risk of COVID-19 infection and the best practices to be followed to stay healthy, as well as providing them relevant and substantiated medical advisories, as per MoHFW and ICMR guidelines, pertaining to the COVID-19 pandemic.

Why should it be used?

Aarogya Setu is our common bridge to prevent the spread of the coronavirus pandemic in India. Aarogya Setu uses contact tracing to record details of all the people we may have come in contact with as we go about your normal activities. If any one of our contacts tests positive for COVID-19, we can be informed and proactive medical facilities can be arranged for us.

In order to break the chain of infection, it is important to provide medical assistance and advice to people who may be at risk, especially asymptomatic people, i.e. people who may have contracted the infection but have not yet shown symptoms.

According to the Govt. of India, Aarogya Setu enabled early identification and prevention of potential risk of infection through contact tracing, and thus acts as a shield for us, our family and our community. In addition, when we take the self-assessment test on the Aarogya Setu app, by correlating the symptoms that we report along with our location information, the Government of India will have the ability to identify hotspots where disease may be spreading, early enough, so that necessary interventions can be done to control and mitigate the spread of COVID-19.

The guidelines by the Government include a directive, which makes it mandatory for all public and private sector office employees to download the Aarogya Setu app. Apart from this, all citizens living in an identified COVID-19 containment zone will also be required to have the Aarogya Setu app installed on their smartphone. The new directive also stated that it will be the responsibility of the heads of the respective organisations, in both private and public offices, to ensure 100 percent coverage of the Aarogya Setu app among employees.

So it is very clear that in the process of curbing Covid-19 pandemic in India with the help of technology Aarogya Setu mobile was created. The very nature of the device was to physically track each individual user, their movement and location. This came in contradiction with IT Acts established under the Indian constitution and overtook the Right to Privacy substantiated as a fundamental right by a nine-judge bench of the Supreme Court headed by Chief Justice JS Khehar, ruled on August 24, 2017, saying that the Right to Privacy is a fundamental right for Indian citizens under the Constitution of India (mostly under Article 21 and additionally under Part III rights). Thus validating that no legislation passed by the government can unduly violate it.

2. OBJECTIVE AND SCOPE

This Article explains how Aarogya Setu was introduced during Covid-19 pandemic its uses and policies that mentions storing and protecting personal user data for Covid-19 protection but it has been heavily criticized and has been referred as a surveillance tool by the Govt. of India. The article explains Aarogya setu's transformation from closed to open source and legalities it covers in reference to Right to privacy and Disaster Management Act 2005.

3. METHODOLOGY

Explorative

4. REVIEW OF LITERATURE

a. IT Act-2008

b. Disaster Management Act -2005

c. The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020

d. Justice K. S. Puttaswamy v. Union of India – Right To Privacy

5. PRIVACY POLICY –AAROGYA SETU APP (2nd April – 26th May, 2020)

When we use Aarogya Setu (App), some personal information is collected from and about us. They mention that they are committed to protecting the security of this information and safeguarding our privacy. This privacy policy sets out the details of the personal information collected, the manner in which its collected, by whom as well as the purposes for which it is used. At registration we also accepted the terms of this Privacy Policy and our use of the App signifies our continued acceptance of its policy thereof. They have explicitly mentioned that their Privacy Policy may be revised from time to time and we will be notified of all such changes. In order to use the App, we will be required to consent to the terms of the Privacy Policy as revised from time to time.

1. Information Collected And Manner Of Collection
a. When we register on the App, the following information is collected from us and stored securely on a server operated and managed by the Government of India (Server) –

(i) name

(ii) phone number

(iii) age

(iv) sex

(v) profession

(vi) countries visited in the last 30 days.

This information will be stored on the Server and a unique digital id (DiD) will be pushed to our App. The DiD will thereafter be used to identify us in all subsequent App related transactions and will be associated with any data or information uploaded from the App to the Server. At registration, our location details are also captured and uploaded to the Server.

b. When two registered users come within Bluetooth range of each other, their Apps will automatically exchange DiDs and record the time and GPS location at which the contact took place. The information that is collected from our App will be securely stored on the mobile device of the other registered user and will not be accessible by such other user. In the event such other registered user tests positive for COVID-19, this information will be securely uploaded from his/her mobile device and stored on the Server.

c. Each time we complete a self-assessment test the App will collect our location data and upload it along with the results of our self-assessment and our DiD to the Server.

d. The App continuously collects our location data and stores securely on our mobile device, a record of all the places we have been at 15 minute intervals. This information will only be uploaded to the Server along with our DiD in (i) if we test positive for COVID-19; and/or (ii) if our self-declared symptoms indicate that we are likely to be infected with COVID-19; and/or (iii) if the result of our self-assessment test is either YELLOW or ORANGE. For the avoidance of doubt, this information will NOT be uploaded to the Server if we are not unwell of if the result of our self-assessment test is GREEN.

e. If we have tested positive for COVID-19 or if there is a high likelihood of us being infected, we have the option to press the Report button on the App which will allow us to either request a test or report that we have tested positive for COVID-19. When we press the Report button the data collected under Clauses 1(b) and (d) and securely stored on our device will be uploaded to the Server with our consent.

2. Use of Information
a. The personal information collected from us at the time of registration under Clause 1(a) above, will be stored on the Server and only be used by the Government of India in anonymized, aggregated datasets for the purpose of generating reports, heat maps and other statistical visualisations for the purpose of the management of COVID-19 in the country or to provide us general notifications pertaining to COVID-19 as may be required. Our DiD will only be co-related with our personal

information in order to communicate to us the probability that we have been infected with COVID-19 and/or to provide persons carrying out medical and administrative interventions necessary in relation to COVID-19, the information they might need about us in order to carry out such interventions.

b. The information collected from any other user's mobile device and uploaded and stored on the Server in accordance with Clause 1(b) will be used to calculate our probability of having been infected with COVID-19.

c. The information collected under Clause 1(c) will be used by the Government of India to evaluate, based on the self-assessment tests and the GPS locations from where they are being uploaded, whether a disease cluster is developing at any geographic location.

d. The information collected under Clause 1(d) and securely uploaded and stored on the Server will, in the event we have tested positive for COVID-19, be used to map the places we visited over the past 30 days in order to identify the locations that need to be sanitised and where people need to be more deeply tested and identify emerging areas where infection outbreaks are likely to occur. Where, in order to more accurately map the places we visited and/or the persons who need to be deeply tested, our personal information is required, the DiD associated with the information collected under Clause 1(d) will be co-related with our personal information collected under Clause 1(a).

e. The information securely uploaded and stored on the Server under Clause 1(e) will be used to calculate the probability of those who have come in contact with us being infected with COVID-19. f. The information collected under Clause 1 will not be used for any purpose other than those mentioned in this Clause 2.

3. Retention
a. All personal information collected from us under Clause 1(a) at the time of registration will be retained for as long as our account remains in existence and if any medical or administrative interventions have been commenced under Clause 2, subject to Clause 3(b) below, for such period thereafter as is required for such interventions to be completed.

b. All personal information collected under Clauses 1(b), 1(c), 1(d) and 1(e) will be retained on the mobile device for a period of 30 days from the date of collection after which, if it has not already been uploaded to the Server, will be purged from the App. All information collected under Clauses 1(b), 1(c), 1(d) and 1(e) and uploaded to the Server will, to the extent that such information relates to people who have not tested positive for COVID-19, will be purged from the Server 45 days after being uploaded. All information collected under Clauses 1(b), 1(c), 1(d) and 1(e) of persons who have tested positive for COVID-19 will be purged from the Server 60 days after such persons have been declared cured of COVID-19. **c.** Nothing set out herein shall apply to the anonymized, aggregated datasets generated by the personal data of registered users of the App or any reports, heat maps or other visualization created using such datasets. Nothing set out herein shall apply to medical reports, diagnoses or other medical information generated by medical professionals in the course of treatment.

4. Rights
a. As a registered user, we have the right to access our profile at any time to add, remove or modify any registration information that we have supplied.

b. We cannot manage the communications that we receive from us or how we receive them. If we no longer wish to receive communications from them, we may cancel our registration. If we cancel our registration, all the information we had provided to us will be deleted after the expiry of 30 days from the date of such cancellation.

5. Data Security
The App is equipped with standard security features to protect the confidentiality and security of our information. Data is encrypted in transit as well as at rest. Personal information provided at the time of registration is encrypted before being uploaded to the cloud where it is stored in a secure encrypted server. Personal information that is stored in the Apps of other registered users that we come in contact with is securely encrypted and are incapable of being accessed by such user.

6. Disclosures And Transfer
Save as otherwise set out in Clause 2 with respect to information provided to persons carrying out medical and administrative interventions necessary in relation to COVID19, no personal information collected by the App will disclosed or transferred to any third party.

6.   THE AAROGYA SETU DATA ACCESS AND KNOWLEDGE SHARING PROTOCOL, 2020
The government of India through its ministry of Electronics and Information technology on 11th May.2020 notified The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020. Under the purview of Disaster Management Act,2005 it constituted Empowered Groups which will identify problem areas and provide effective solutions, delineate policy, formulate plans, strategise operations and take all necessary steps for effective and time bound implementation of these plans/policies/strategies/decisions in relation to the Covid-19 pandemic and functioning of Aarogya Setu mobile application and data management and for effective operation to detect and mitigate spread of Covid-19. Also in order to ensure secure collection of data by Aarogya Setu mobile application, protection of personal data of individuals and the efficient use and sharing of personal or non-personal data for mitigation and redressal of Covid-19 The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 has been formed.

1. Rationale for this Protocol
1. Owing to the COVID-19 pandemic, guidelines have been issued by the Ministry of Home Affairs (vide Orders dated 24.03.2020, 25.03.2020, 28.03.2020, 1.04.2020, 2.04.2020, 14.04.2020, 16.04.2020, 1.05.2020) on the measures to be taken by the Central Government as well as the State/Union Territory Governments. Various advisories and statements have been issued by the Ministry of Health and Family Welfare, Government of India and other Ministries of the Government of India and State/ Union Territory Governments on precautionary measures such as social distancing and treatment of individuals who are affected or at-risk. In order to ensure their effective implementation, there is a need to ensure efficient data and information sharing among the different Departments and Ministries of the Government of India as well as those in the State/Union Territory Governments.

2. At present, the Government of India and State/Union Territory Governments are tasked with formulating appropriate health responses to not only contain the epidemic but also protect the health and safety of the community at large. Here, appropriate health responses include prevention and management of the COVID-19 pandemic, syndromic mapping, contact tracing, communication to an affected or at-risk individual's family and acquaintances, performance of statistical analysis, medical research, formulation of treatment plans or other medical and public health responses related to the redressal and management of the COVID-19 pandemic.

3. In order to formulate appropriate health responses for addressing the COVID-19 pandemic, data pertaining to individuals is urgently required. Here individuals mean persons who are infected, at high risk of being infected or who have come in contact with infected individuals. This data includes demographic data, contact data, self assessment data and location data (collectively called 'response data' in this document). Here, demographic data means the name, mobile number, age, gender, profession and travel history of an individual. Contact data means data about any other individual that a given individual has come in close proximity with, including the duration of the contact, the proximate distance between the individuals and the geographical location at which the contact occurred. Self assessment data means the responses provided by that individual to the self assessment test administered within the Aarogya Setu mobile application. Location data means data about the geographical position of an individual in latitude and longitude.

4. Implementation of the Protocol:
Keeping in view of the above, the Ministry of Electronics and Information Technology, Government of India ("MeitY") is designated as the agency responsible for the implementation of this Protocol and its developer, the National Informatics Centre shall, under this Protocol be responsible for collection, processing and managing response data collected by the Aarogya Setu mobile application. Any reference to MeitY under this Protocol is a reference to its supervisory role in relation to the Aarogya Setu mobile application and its developer, the National Informatics Centre (NIC) and not in any other

capacity. For the purpose of this Protocol, MeitY shall act under the overall direction of the Empowered Group 9 on Technology and Data Management.

5. Principles For Collection And Processing Of Response Data:

a. Any response data and the purpose for which it is collected by NIC shall be clearly specified in the Privacy Policy of the Aarogya Setu mobile application. b. NIC shall collect only such response data as is necessary and proportionate to formulate or implement appropriate health responses. Further, such data shall be used strictly for the purpose of formulating or implementing appropriate health responses and constantly improving such responses. c. NIC shall process any data collected by it in a fair, transparent and non-discriminatory manner. d. Contact and location data shall by default, remain on the device on which the Aarogya Setu mobile application has been installed after such data has been collected. It may be uploaded to the server only for the purpose of formulating or implementing appropriate health responses. e. Contact, location and self assessment data of an individual that has been collected by NIC shall not be retained beyond the period necessary to satisfy the purpose for which it is obtained which, unless a specific recommendation to this effect is made in the review under Para 10 of this Protocol, shall not ordinarily extend beyond 180 days from the date on which it is collected, after which such data shall be permanently deleted. Demographic data of an individual that has been collected by NIC shall be retained for as long as this Protocol remains in force or if the individual requests that it be deleted, for a maximum of 30 days from such request, whichever is earlier. f. The response data shall be securely stored by NIC and shall only be shared in accordance with this Protocol.

6. Principles for Sharing Of Response Data:

The response data may be shared by NIC in the following manner:

a. Response data containing personal data may be shared with the Ministry of Health and Family Welfare, Government of India, Departments of Health of the State/Union Territory Governments/ local governments, NDMA, SDMAs, such other Ministries and Departments of the Government of India and State Governments and other public health institutions of the Government of India, State Governments and local governments, where such sharing is strictly necessary to directly formulate or implement an appropriate health response.

b. Response data in de-identified form may be shared with such Ministries or Departments of the Government of India or the State/Union Territory Governments, local governments, NDMA, SDMAs and such other public health institutions of the Government of India or State Governments or local governments with whom such sharing is necessary to assist in the formulation or implementation of a critical health response. Here, de-identified form means data which has been stripped of personally identifiable data to prevent the individual from being personally identified through such data and assigned a randomly generated ID.

c. NIC shall, to the extent reasonable, document the sharing of any data and maintain a list of the agencies with whom such data has been shared. Such documentation shall include the time at which such data sharing was initiated, the persons or agencies who are being provided access to such data, the categories of data that are being shared and the purpose for which such data is being shared.

7. OBLIGATIONS OF ENTITIES WITH WHOM RESPONSE DATA IS SHARED:

a. An entity with whom response data is shared under this Protocol shall have the following obligations: a. Any entity with whom response data has been shared under Para 6 of this Protocol shall use such data strictly for the purpose for which it is shared. Such Ministry, Department of the Government, NDMA, SDMAs or public health institution shall process response data in a fair, transparent and non-discriminatory manner. The data accessed and used by such entities should not be retained beyond the period necessary to satisfy the purpose for which it is shared. In any circumstance, such data shall not ordinarily be retained beyond 180 days from the date on which it was accessed, after which such data shall be permanently deleted. Any Ministry, Department of the Government, NDMA, SDMAs or public health institution shall also implement reasonable security practices and procedures as prescribed under any law for the time being in force.

b. Any response data accessed under para 7(a) shall ordinarily not be onward shared with any third party. However, response data may be shared with such third parties only if it is strictly necessary to

directly formulate or implement appropriate health responses. The Ministry or Department of the Government of India or State/ Union Territory Government/ local government, NDMA, SDMAs or public health institution of the Government of India/ State Governments/ local governments referred to in Para 6 that is sharing such information shall remain responsible for adherence to this Protocol by any other entity with which it shares information. Any third party with whom data is onward shared under this para shall be subject to the same obligations as under para 7(a) of this Protocol. In addition they shall not re-use the data for any other purpose or disclose the data to any other entity and remain subject to audit and review of their data usage by the Central Government.

8. PRINCIPLES FOR SHARING OF RESPONSE DATA FOR RESEARCH PURPOSES

Response data may be made available for research purposes by NIC in the following manner: **a.** Hard anonymisation refers to a series of technical processes which ensure that any individual is incapable of being identified from the response data through any means reasonably likely to be used to identify such individual. This anonymisation shall be done in accordance with anonymisation protocols that are to be developed, reviewed and updated on a periodic basis by an expert committee appointed by the Principal Scientific Advisor to the Government of India. Such review shall have regard to the nature and sensitivity of the data being processed, the robustness of the anonymisation protocol and advances in technology.

b. Response data which has undergone hard anonymisation, as under para 8(a), may be made available to Indian universities and research institutions / research entities registered in India. **c.** Any university or research institution / entity seeking to access response data under para 8(b) shall make a request for such data to the expert committee referred above at para 8(a), who may approve of such request and provide access to this data only if it is of the view that such access is sought for the purposes of statistical, epidemiological, scientific or any other form of academic research, on such terms as may be stipulated by the expert committee in this behalf.

d. Any university or research institution/ entity which accesses anonymised response data under Para 8(b) shall not reverse anonymise such data or re-identify individuals in any manner. If any person knowingly or unknowingly, takes any action which has the effect of such data no longer remaining anonymised, any rights granted to them under this Protocol shall stand terminated, and they shall be liable for penalties under applicable laws for the time being in force.

e. Any university or research institution/ entity which accesses anonymised response data under this Para may share such anonymised response data with other Indian universities or research institutions/ research entities registered in India only if such sharing is in furtherance of the same purpose for which it has sought approval to access such data from the expert committee. Any such third party with whom data is shared under this Para shall be subject to the same obligations and penalties under this Protocol as the university/ research institution/ entity which has shared the data with it. Any such sharing must be pursuant to a contract between the two entities, which shall state the nature of data shared, the purpose of such sharing, the duration of such sharing and other relevant details as may be specified by the expert committee. Such contracts, intimation of the fact of sharing and other relevant documentation as may be specified by the expert committee shall be submitted by the approved university/ research institution/ entity to the expert committee for review and compliance.

f. Any university/ research institution/ entity with whom hard anonymised data has been shared under Para 8(a) or Para 8(e) shall remain subject to audit and review by the Central Government. Further, if the Expert Committee finds any non-compliance with this protocol by such university/ research institution/ entity, it can terminate any rights granted to them under this Protocol at any time.

9. Violations

Any violation of these directions may lead to penalties as per section 51 to 60 of the Disaster Management Act, 2005 and other legal provisions as may be applicable.

10. Sunset Clause

The Empowered Group shall review this Protocol after a period of 6 months from the date of this notification or may do so, at such earlier time as it deems fit. Unless specifically extended by the

Empowered Group on account of the continuation of the COVID-19 pandemic in India, this Protocol shall be in force for 6 months from the date on which it is issued.

9. Policy Explanation in General

According to mentioned protocol, the response data containing personal data may be shared by the National Informatics Centre (NIC) – with The Ministry or Department of the Government of India or State/ Union Territory Government/ local government, NDMA, SDMAs or public health institution of the other Ministries and Departments of the Government of India and State Governments and other public health institutions of the Government of India, State Governments and local governments, where such sharing is strictly necessary to directly formulate or implement an appropriate health response. Response data may also be shared with Indian universities or research institutions and research entities registered in India for research purposes.

The Protocol states that response data in de-identified form may be shared with such Ministries or Departments of Government of India or Government of the State / Union Territory Governments, local governments, NDMAs, SDMAs and other public health institutions of the Government of India or Governments of the State.

De-identified form means data that has been stripped of personally identifiable data to prevent the individual from being directly identified through such data and they are assigned a randomly generated ID for maintaining their anonymity.

7. Criticisms

a. Threat to Right to Privacy: Aarogya Setu stores location data and requires constant access to the Bluetooth phone, which, experts say, makes it invasive from a security and privacy point of view.

b. Limited liability: The liability clause exempts the Government from liability in any event of "any unauthorized access to the user's information or modification thereof," simply there is no liability for the Government even if the personal information of users is leaked.

c. Transparency : Other contract tracing app from countries such as UK's Covid-19 tracing app, The Aarogya Setu App was not open source, which meant that it cannot be audited for security flaws by independent coders and researchers

d. Prejudice: There were various reports on the social media and lots of fake news that questioned the very nature of Aarogya Setu App as tool for surveillance and data collection for indirect National Population Register (NPR) and NCR as well.

8. Open Source and its future

As on 26th May 2020, Ministry of Electronics & Information Technology declared Aarogya Setu as an Open Source project. The ministry notification said that the key pillars of Aarogya Setu have been transparency, privacy and security and in line with India's policy on Open Source Software, the source code of Aarogya Setu has been made open source.

The source code for the Android version of the application has been made available for review and collaboration at github.

The iOS version of the application will be released as open source within the next two weeks and the server code will be released subsequently. Almost 98% of Aarogya Setu Users are on Android platform.

1. Bug Bounty Programme

While making the code Open Source, Government of India also seeks the developer community to help identify any vulnerabilities or code improvement in order to make Aarogya Setu more robust and secure. To fulfil this objective, Government has also launched a Bug Bounty Programme with a goal to partner with security researchers and Indian developer community to test the security effectiveness of Aargoya Setu and also to improve or enhance its security and build user's trust by making the app processes transparent.

This massive Bug Bounty Programme is open till 26th June,2020 and promises prize money ranging from one lakh to thirty lakhs for identifying and rectifying Security Vulnerability in the app.

9. APP STATISTICS AND SUCCESS

The App may have the most impact and reach compared to all other COVID-19 contact tracing and self-assessment tools combined globally, while pioneering new data led resolution to one of the most impactful calamity of the modern era. Out of 114 million registered users, two-thirds have taken the self-assessment test to evaluate their risk of COVID-19 exposure. The App helped identify about 500,000 Bluetooth contacts. Those identified as positive Bluetooth contacts of COVID-19 or classified as needing assistance on the basis of their self-assessment are contacted by the National Health Authority. So far, the platform has reached out to more than 900,000 users and helped advise them for Quarantine, caution or testing. Among those recommended for COVID19 testing, it was found that almost 24 percent of them were found to be positive for COVID-19. Compare this to the average positive result of COVID-19 of about 4.65 per cent-145380 COVID-19 positive from a total of 3126119 experiments carried out on 26 May 2020.

Apart from that as claimed the app also became an authentic source of information regarding the Covid-19 pandemic and removed many misconceptions from the minds of the people. "Kb, Sankaranarayanan. (2020). A study on "Arogya Setu" Application as counterfeit to COVID- 19: False News circulation in Social Media. 10.13140/RG.2.2.22613.99040."

10. CONCLUSION

The app did reach out to more than 900,000 users and helped advise them for Quarantine, caution or testing. About 4.65 percent i.e 145380 COVID-19 positive from a total of 3126119 experiments by 26 May 2020 showed the apps utility during the pandemic. But as every individual of the society we all have rights documented by the constitution of India, which guarantees each individual his/her, private space for whichever activity (considering that the activities are legal).
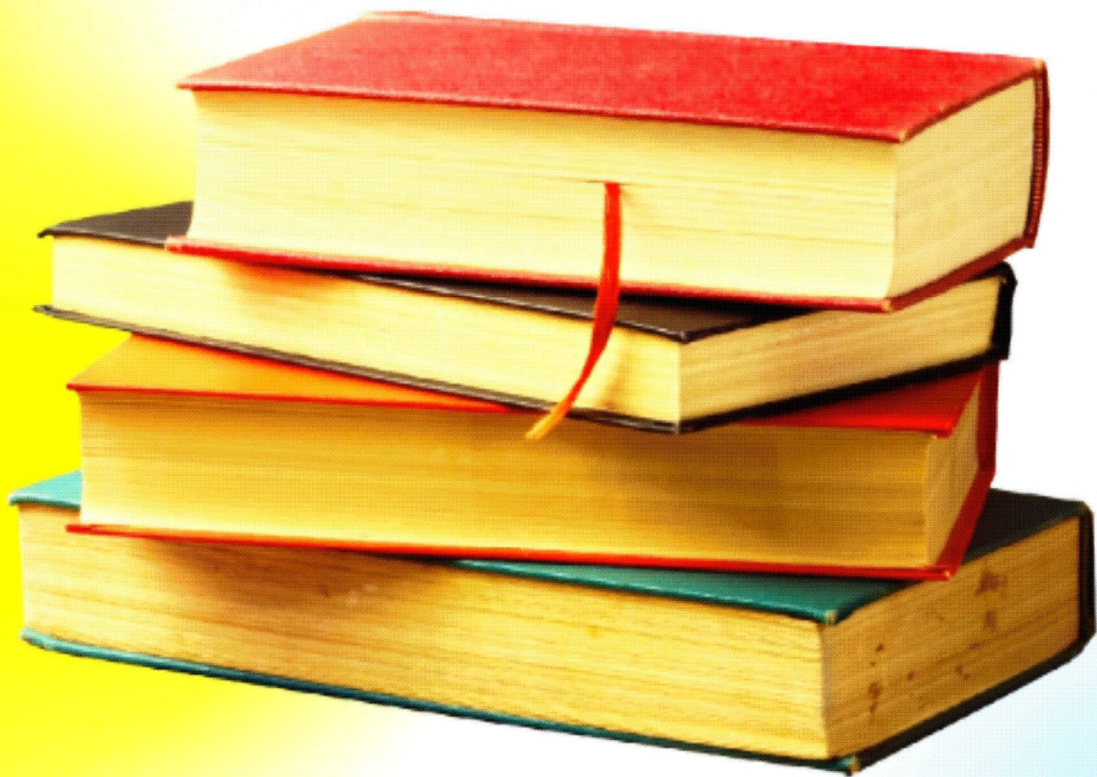
Any app that tracks who you have been in contact with and your specific location with pin point accuracy at all times is a clear violation of our privacy rights. The somewhat vague and lose nature of the protocol and framed policies is also a concern. Considering India's horrible past with protecting data privacy, one of the main concerns with this app is sharing of this private data with third-party entities. Our inefficient IT Act and the still hypothetical privacy and data protection bill provide not much hope. It was undoubtedly a failure of the constitutional machinery and the protection of fundamental rights was not addressed properly. After 55 days of launch the open source conversion of the Aarogya Setu App has been one of the most required decisions taken by the Government of India. This finally made the contact tracing process of the app transparent and helped to rebuild and restore the trust of common individual into the constitutional machinery that has been put in place to safeguard his/her interests and rights. Moreover the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 also specified that the app collected data will at most be used for six months. Though the Aarogya Setu App is now open source the responsibility of the government to use technology for our benefits during the Covid-19 pandemic is far from over. The in adequate privacy policy, the misuse of Disaster Management Act 2005 for sensitive data collection and third party sharing of data is still a ghost which haunts us. Even during an emergency situation we hope that next time whenever someone from us installs or selects any government driven application, we do it with trust and confidence.

REFERENCES

- https://static.mygov.in/rest/s3fs-public/mygov_159051645651307401.pdf

- https://static1.swaraksha.gov.in/tnc/

- https://static1.swaraksha.gov.in/privacy/

- https://static.mygov.in/rest/s3fs-public/mygov_159051652451307401.pdf

- https://indiankanoon.org/doc/127517806/

- https://github.com/nic-delhi/AarogyaSetu_Android.git.

- https://static.mygov.in/rest/s3fs-public/mygov_159050690151307401.pdf

- https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1626979

- https://www.orfonline.org/expert-speak/aarogya-setu-app-many-conflicts-67442/
- https://internetfreedom.in/is-aarogya-setu-privacy-first-nope-but-it-could-be-if-the-government-wanted/

Studies in Indian Place Names (SIPN) with ISSN 2394-3114