Evaluation of COVID-19 tracking mobile application of India

Abhishek Royal[1*], Mohammad Atif Aleem[2]

[1]Universitas Gadjah Mada, Indonesia; [2]Tata Consultancy Services, India

*Correspondence: abhishekroyal2010@gmail.com

Abstract

Background: Use of mobile location data is emerging as one of the major strategy to guide public health interventions to contain the spread of COVID-19 across the globe. The paper intends to explore and evaluate the issues associated with Aarogya Setu, COVID-19 tracking mobile application of India.

Methods: The study comprises of security testing of Android version of mobile application, its assessment from users' perspectives and in-depth exploration from experts' opinion. The results are triangulated with the literature review, open editorial articles, published statements and opinions.

Results: The automated security testing reported 3 medium level, 3 low level and no high level risks in Android version 1.1.1 and reported 5 medium level, 4 low level and no high level risks in version 1.4.1. The audit also reported 7 warnings for both these versions. The mean of users' mean app quality score for Aarogya Setu is estimated to be 12.145 (95% CI; 11.61 – 12.67). The deductive thematic analysis of experts' opinion reported concerns related to in-built disclosures, human rights, data security and privacy, policy and legal perspectives.

Conclusion: The vulnerabilities in the mobile app and weak policy on the data security in India need to be addressed for successful implementation and adoption of this digital intervention.

Keywords: Mobile Tracking App, COVID19, Aarogya Setu, India, Data security, Health informatics

Introduction

The current pandemic of COVID-19 has overwhelmed the entire world. The disease was first identified in Wuhan, China in December 2019. The World Health Organization (WHO) identified this outbreak as Public Health Emergency of International Concern (PHEIC) on 30th January 2020 and declared it as a 'pandemic' on 11th March 2020. A total of 30,949,804 cases have been reported with 959,116 deaths till 21st September, 2020 (05:30 GMT) across the globe. Around 235 countries, areas or territories have reported cases till now (1,2).

Contact tracing helps in identification of individuals exposed to diagnosed cases and aids to quarantine, test and treat them in case of development of symptoms. It helps in breaking the chain of human to human transmission and is considered as an important component of comprehensive strategies to control the spread of COVID-19 (3). The traditional contact tracing systems face a wide range of challenges including incomplete identification of contacts, inefficiency of paper-based reporting systems, complexity of data management and delays in identification of contacts and initiating their quarantine and isolation. Digital tools are playing a significant role in overcoming these challenges and ensuring the proper and effective integration of contact tracing in to public health systems (4). These digital contact tracing tools can be classified in to outbreak response tools, proximity tracing tools and symptom tracking tools.

Outbreak response tools are designed for public health personnel involved in contact tracing activities in outbreak investigations. These tools allow tailored case investigations, contact listing and their follow ups and are useful for initial localized outbreak response and early cluster investigations in limited populations. *Proximity tracing tools* use GPS location or Bluetooth technology to trace the movements of the users to identify the individuals who have been exposed to an infected person. These tools can be categorized as either centralized (contact history processed centrally by a health authority) or decentralized (contact history processed by individual devices). There are concerns about the disclosure of personal data in these tools and these privacy issues should be addressed before wide implementation of these tools (5). *Symptom tracking tools* routinely collect self reported data on signs and symptoms of the disease to understand its severity or ascertain the probability of the infection (6).

Use of mobile location data is emerging as one of the major strategy to guide public health interventions to contain the spread of COVID-19 across the globe. The countries are promoting mobile applications to track movement and spread of infection, thereby formulating risk routes travelled by recently diagnosed cases to warn the exposed individuals to get tested and quarantine to break the chain of transmission. According to a tracking conducted by MIT Technology Review, around 50 governments have currently implemented COVID-19 tracing apps (7).

The Government of India (GoI) launched a mobile application to augment its initiatives to control the spread of COVID-19 on 2nd April 2020. The Aarogya Setu mobile application aims to

inform people about their potential risk, best practices to stay healthy and provide them information on relevant and updated advisories issued by Ministry of Health and Family Welfare (MoHFW) and ICMR (Indian Council of Medical Research) related to COVID-19 pandemic. The 'Aarogya Setu' mobile application can be downloaded from PlayStore (for Android devices), AppStore (for iOS devices) or the Jio Appstore (KaiOS). The salient features of the application includes self-assessment test, risk status of the user, automatic contact tracing using Bluetooth, geo-location based COVID-19 statistics and; updates, advisory and best practices related to COVID-19. The application is supported in 12 languages (as per 26th May 2020) and also enlists emergency helpline contacts and ICMR approved labs for COVID-19 testing facilities (8). The source code of Aarogya Setu was made open source on 26th May 2020 after the registration of 114 million users. The source code for the Android version is available at https://github.com/nic-delhi/AarogyaSetu_Android.git for review and collaboration (9).

The Aarogya Setu server assigns a random unique device identity number (DiD) and associates it with the registered mobile number. The app detects other devices in the Bluetooth proximity with the same application. The interaction results in secure exchange of a digital signature including time, location, proximity and duration of contact. The application calculates the risk of infection and recommends suitable action which is displayed on user's Home screen. The updated risk of infection is analysed by GoI to facilitate medical interventions (8). In the event of positive test results, the testing laboratory shares this information with ICMR which further shares the list of COVID-19 positive persons with the Aarogya Setu server. The server updates the status of the user in the application and runs contact tracing for this person. The Home screen of the application also shows statistics of number of users who have been tested COVID-19 positive or come in direct contact with someone tested positive from an individual's location at a distance of 500m, 1km, 2km, 5km and 10km.

The use of these mobile applications has been voluntary, non-compulsory, and compulsory and even enforced depending on the country of implementation. India is the only democracy making its COVID-19 tracing application mandatory for millions of people (7). Due to intensive Information, Education and Communication (IEC) activities and endorsements, the app has witnessed over 100 million installs by 13th May 2020. However, various concerns have been reported related to the data security and lack of effective safeguards to protect privacy of the users in this application. This paper intends to explore and evaluate the Aarogya Setu mobile application from multiple perspectives including privacy, data security, legal, policy and human rights.

Methods

A review of literature on the data security and privacy issues related to mobile tracking apps in COVID-19 was performed. Since there is dearth of availability of the studies on the use of mobile application in current pandemic in global context in general and Indian context in

particular, the available open editorial articles, statements and endorsements of civil society organizations and experts' comments were also included in the literature search.

The Android version of the mobile application (App ID: nic.goi.aarogyasetu) was scanned through ImmuniWeb ® Community Mobile App Security Test, an open source Dynamic Application Security Testing Tool to check for security vulnerabilities. This testing includes security testing of mobile application, its backend (eg. web services or APIs that send or receive data from the app) and the encryption between them (10). The version 1.1.1 of the mobile application was tested on 19th May 2020 followed by a re-testing of the updated version 1.4.1 on 1st September 2020. A comparative analysis of the results of these versions was conducted for the risks and warnings reported during the security testing.

An open survey was conducted to obtain users' feedback on the quality of Aarogya Setu mobile application. The user version of Mobile Application Rating Scale (uMARS) was converted in to a Google form and sent to 120 participants selected through purposive sampling via email and Whatsapp in the first week of September 2020. The uMARS is developed from the original version of MARS tool that was developed for Wellbeing Project as a partnership between Queensland University of Technology and the Young and Well Cooperative Research centre. The uMARS is a 20-item pre-validated tool with 4 objective quality subscales: engagement, functionality, aesthetics, and information quality; and a subjective quality rating. This scale also assess the perceived impact of the mobile application in 6 domains: awareness, knowledge, attitudes, intention to change, help seeking and behaviour change (11). The responses were analyzed in MS Excel 2007 and StataMP 14.

A total of 6 experts in the field of Data Privacy, Cyber-security, Information Technology, Mobile Application Development, Law and Human Rights, who have used the mobile application were identified and were contacted for their opinions about Aarogya Setu mobile application. An open ended, semi-structured questionnaire covering broad themes related to in-built disclosures of the application, its technology platform and usage, concerns related to data security and privacy of Application, the policy and legal perspectives were administered to these experts. A deductive thematic analysis of the responses was conducted to extract relevant themes, codes and opinions and presented in this paper.

The findings of the security testing, users' survey and experts opinion were triangulated with literature search and presented in this paper.

Results

The Aarogya Setu mobile application collect following information at the time registration: name, phone number, age, sex, profession and countries visited in the last 30 days. The application has four sections: 1) **Your Status**: inform the users about their risk of getting infected with COVID-19; 2) **Self Assess**: inform about the risk of being infected; 3) **COVID-19**

updates: updates on local, regional and national cases and; 4) **E-pass**: e-pass available if applied for movement in lockdown. It asks permission to access location (network-based approximate location and GPS/ network-based precise location). The other permissions include permission to receive data from internet, view network connections, access Bluetooth settings and pair with Bluetooth devices, full network access, run at the start up and prevent device from sleeping.

1. Security testing for the mobile application

1.1 Assessment of Aarogya Setu Mobile Application (Version 1.1.1)

The Android version 1.1.1 of the mobile application was scanned on 19th May 2020 at 23:01 CDT through ImmuniWeb ® Community Mobile App Security Test. The automated audit reported 3 medium risks (Table 1), 3 low risks (Table 2) and 7 warnings for this version and no high risk security flaws were reported.

Table 1. Medium Risk Security Flaws and Weaknesses in Aarogya Setu Version 1.1.1

S.No.	Risks	Description
1.	Weak Encryption	Badly implemented or weak encrypted algorithms can endanger data transmission and storage.
2.	Usage of unencrypted HTTP protocol	This version uses HTTP protocol to send and receive data. The current design of HTTP protocol does not provide any encryption of the transmitted data. This can be easily intercepted if an attacker is located in the same network.
3.	Predictable random number generator (RNG)	This version uses predictable Random Number Generator. This may jeopardize data encryption or other protection based on randomization of the mobile application. This may result in execution of a sensitive activity within the application and its backend by an attacker by providing a predictable token for validation.

Table 2. Low Risk Security Flaws and Weaknesses in Aarogya Setu Version 1.1.1

S. No.	Low Risk	Description
1.	Hardcoded data	This version contains debugging or other technical information that may be extracted and used by an attacker to facilitate further attacks.
2.	Missing Tapjacking protection	This version do not have tapjacking protection to mitigate attacks. Android OS permits a mobile application to display its user interface over the user's interface of

		another installed running application on the mobile. This may allow passing of the touch event to another application below its user interface. The malicious application may exploit this tendency as a proxy to pass unintended touch for various forms of exploitations.
3.	Exported broadcast receivers	The version of this mobile application contains an exported receiver enabling other applications to send intents without any restrictions. This can be exploited by malicious applications to send intents to mobile application's broadcast receiver.

1.2 Assessment of Aarogya Setu Mobile Application (Version 1.4.1)

The updated version (Android version 1.4.1) of Aarogya Setu mobile application was scanned on 1st September 2020 at 00:18 hours CDT through ImmuniWeb ® Community Mobile App Security Test to assess the recent version for the updates and interventions. The automated audit revealed 5 medium risks (Table 3), 4 low risks (Table 4) and 7 warnings while no high risk security flaw and weakness was reported. The detailed original report is presented in Appendix 2.

Table 3. Medium Risk Security Flaws and Weaknesses in Aarogya Setu Version 1.4.1

S.No.	Risks	Description
1.	External Data in Raw SQL Queries	The inclusion of inputs in to raw SQL queries can potentially lead to the injection of local SQL vulnerability in current version of this mobile application.
2.	Weak Encryption	The weakness is not rectified in the current version of the mobile application
3.	Usage of unencrypted HTTP protocol	The current version still uses HTTP protocol to send and receive data. The weakness has not been resolved in the updated versions.
4.	Predictable random number generator (RNG)	The current version still uses Random Number Generator.
5.	Clear Text SQLite Database	The version uses an unencrypted SQLite database. This database can be accessed by an attacker with physical access to the mobile device or a malicious application with root access to the device. It is recommended for the application to not store sensitive information in clear text.

Table 4. Low Risk Security Flaws and Weaknesses in Aarogya Setu Version 1.4.1

S. No.	Low Risk	Description
1.	Hardcoded data	The current version still contains debugging or other technical information that may be extracted and used by an attacker to facilitate further attacks.
2.	Missing Tapjacking protection	The current version still does not have tapjacking protection to mitigate attacks.
3.	Exported broadcast receivers	The current version still contains an exported receiver enabling other applications to send intents without restrictions.
4.	Exposure of potentially sensitive data	The current version has the tendency to expose potentially sensitive information during its run times.

Warnings: The warnings reported in the analysis remained same for both the analyzed versions. The analysis reported following seven warnings in these versions of the mobile application:

1) Both versions of the mobile application create temporary files. It is recommended to securely delete the temporary files when not required by the application.

2) Both versions use 'implicit intent' that may be insecure under certain conditions**.** 'Intents' enables mobile applications to communicate with each other by sending requests to perform an action. The implicit intent does not specify the applications that it can send request to perform actions. This weakness can be utilized by malicious applications to receive implicit intent and perform actions.

3) These versions use an intent filter which may pose a serious security risk if not implemented and filtered properly. Intent filters put no restrictions on explicit intents and developers should not completely rely on intent filters to ensure the security of the mobile application.

4) The versions have enabled JavaScript (JS) in Web View which is disabled by default. If enabled, it can bring various JS-related security issues. eg. XSS attacks (Cross-site scripting).

5) These versions of the mobile application use dynamic load of executable code which can be dangerous in certain conditions. The location of code on external storage can lead to code injection vulnerability if the external storage is readable and/or writable by the world and accessible to the attackers.

6) The versions use weak hashing algorithms. These algorithms are vulnerable to collisions and other security weaknesses. It is recommended to use reliable hashing of data in the case of sensitive data.

7) The object de-serialization is performed on a non-trusted resource for both the versions. This can be dangerous if the data for de-serialization is tempered by an attacker.

The analysis revealed no significant changes in the risks and security flaws between the two analysed versions.

2. Users' Assessment of Aarogya Setu mobile application

Only 101 participants out of 120 filled the survey while 19 participants did not attempt the survey citing the reasons that they have never used the mobile application. Only one of the respondents did not complete the survey and therefore excluded in the final analysis. The final analysis included response from 100 respondents.

Engagement: The mean and median score for engagement component (out of 25) for Aarogya Setu is 12.9 (95% CI 12.17 – 13.63) and 13 respectively. The score range from 5 to 25. 41% of the respondents found this application dull and not entertaining at all. Only 25% found it fun enough to entertain a user for a brief time (< 5 minutes) while 21% found it fun and entertaining for 5 – 10 minutes. 21 out of 100 respondents found it not interesting at all while 30 out of 100 respondents found it interesting (moderately or very interesting). Only 40% of the respondents accepted that the app allows basic customisation of features and 37% reported that it allows basic interactive features to function adequately. The app content (visual information, language, design) is reported acceptable but not targeted (may be unclear/ confusing/ inappropriate) by 58% of the respondents.

Functionality: The mean and median score for functionality component (out of 20) for the mobile application is 12.54 (95% CI 11.89 – 13.19) and 12.5 respectively with a range score of 4 and 19. 63% of the respondents reported that the app is mostly functional with some technical problems that need fixing or minor/ negligible problems and 52% respondents found it easy to learn to use the app. 40% of the respondents found it easy to understand/ navigate between screens and 37% found taps/swipes/pinches/scrolls mostly consistent/ intuitive all across the components/screens with negligible problems.

Aesthetics: The mean and median aesthetics component score (out of 15) for the mobile application is 9.66 (95% CI 9.22 – 10.09) and 10 respectively. The score has a range from 4 to 15. The layout of the app is found to be mostly clear by 43% of the respondents. The graphics and visual design is reported to be of moderate quality by 57% and the visual appeal of the application was found to be average (neither pleasant, nor unpleasant) by 51% of the respondents.

Information: The mean and median score for the information component (out of 20) is 13.48 (95% CI 12.78 – 14.18) and 14 respectively. Only 33% of the respondents found the quality of information to be relevant or coherent or correct and offers a broad range of information with some gaps and unnecessary details. The visual information is found to be mostly clear, logical and correct with negligible issues by 44% of the respondents. 35% of the respondents accept that the information within the app possible comes from a legitimate source.

The mean of users' mean app quality score for Aarogya Setu mobile application is 12.145 (95% CI 11.61 – 12.67) with a range of 4.25 – 19.75 (Table 5). 28% of the respondents will not recommend this app to anyone and only 15% reported to recommend this app to everyone. While 10% of the respondents will not use this app, only 14% will use this app for > 50 times in next 12 months. 3 out of 5 respondents are not interested in paying for this app and only 2% expressed their willingness to pay for this app. 45% of the respondents have star rated this mobile application as average (3 stars) followed by 28% of the respondents who rated it as poor (2 stars).

Table 5. Scoring of Aarogya Setu mobile application through uMARS

Score	Mean	Standard Error	95% Confidence Interval
Engagement Score (Out of 25)	12.9	0.3702	12.1654 – 13.6346
Functionality Score (Out of 20)	12.54	0.3282	11.8886 – 13.1913
Aesthetics Score (Out of 15)	9.66	0.2202	9.2228 – 10.0971
Information Score (Out of 20)	13.48	0.3514	12.7826 -14.1774
App Quality Score (Out of 80)	48.58	1.0708	46.4552 – 50.7048
Mean App Quality Score	12.145	0.2677	11.6138 – 12.6762

Perceived Impact: More than 40 % of the users have disagreed that the mobile application has increased their awareness in addressing the health crisis and only 28% of the users have slightly or completely agreed that the mobile application has increased their knowledge and changed their attitude about the health behaviour in response to the pandemic (Figure 1). 31% of the respondents neither agreed nor disagreed that the app has increased their intention/ motivation to address their health behaviour. 33% of the users has moderately/ strongly agreed that the app has

improved their health seeking behaviour and 31% of the users have moderately/ completely admitted that the app has changed their behaviour about the disease.

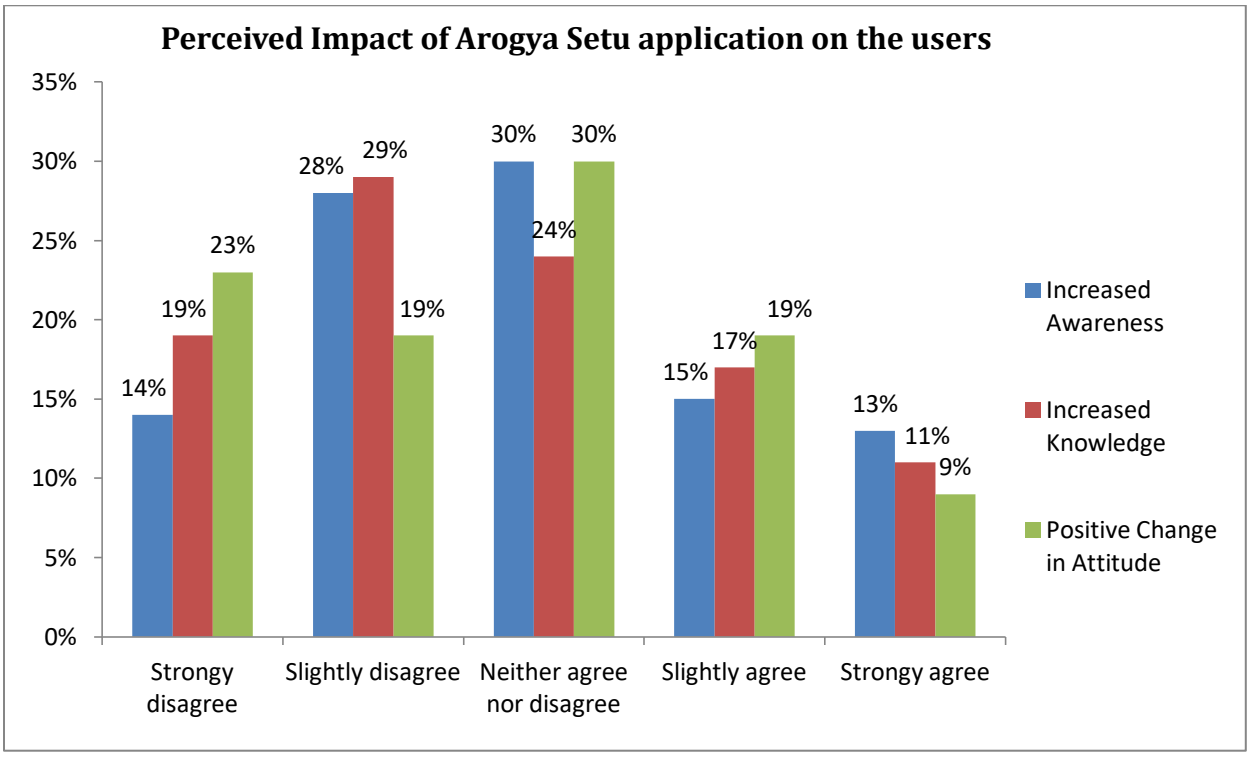

Figure 1. Perceived Impact of Aarogya Setu mobile application on the users

The users also provided mixed comments about the application. Though some of the users reported it to be *good, relevant, and important* and as a *need of the hour*, others reported it to be *average* and suggested for more *improvements/ updates/ revisions.* A user also mentioned that *"using Bluetooth for the entire day can hack the mobile".* Another user who is consistently travelling reported that *"I only use because it is mandatory at airport transits".* A user also shared concerns and mentioned "*figures with only +ve sense have been prioritized to be shown on the screen, which according to me, an irresponsible and zero accountable system…people should be aware of the current situation in all fronts…second major issue is that the nearby positive cases features does not makes any sense... sometimes it shows different figures in different phones located at same co-ordinates".*

3. Assessment of Expert's Opinion

The experts' reached out for opinion aged between 23 to 45 years and working in diverse sectors including international organizations. Their identities were kept anonymous while performing the content analysis and reporting their response. Themes and codes were extracted from their responses and are reported in Table 6.

3.1. Disclosures about Privacy Policy

Most of the experts pointed limitations in disclosures to data and privacy policy. They also cited important aspects of identification of data, privacy policy gaps, purpose identification and how new changes that were not notified to the users is a breach in the mandate of privacy statement.

3.2. Robustness and security aspects of the application

The robustness and security aspect of the application were highlighted by technical experts working in information technology and cyber security sector as being not as adequate as compared to other contact tracing mobile applications in the world. The privacy expert specifically mentioned that there is no consideration to ensure and validate Privacy in the design of the application's architecture, which means that the security aspect has not been looked upon thoroughly by the developers. The experts also pointed that linking of the application with government datasets through servers can be a tool of mass surveillance and can result in violation of privacy of millions of users.

3.3. Opinions on lifespan/ removal of the application as mandated by the government

The lifespan of 180 days for Aarogya Setu app as mandated by the government of India drew criticism from some experts regarding the concept of purpose limitation, methods of erasure, monitoring and implementation challenges while being appreciated by some as being a good decision to abate future references of data.

3.4. Information on availability of source codes of the application in the public domain

The information on availability of codes in the public domain was met with skepticism by majority of the experts with respect to this application, as the codes were made public much after a voice was raised for it and lacked disclosures and robustness. Overall it was deduced that open sourcing is a healthy process and makes transparency and accountability in an easier way. Proactive consultation with industrial specialists, experts and ethical hackers were suggested as a way forward in this regard to improve the usage of the App and to make it more robust. The cyber security expert mentioned that *"releasing them (the codes through open source) earlier would have led to a more inclusive process when it comes to the development of the app. Probably would have helped to moderate the debate around its privacy and security features as well".* Thus, making the codes of the application available in the public domain is important and can lead to consultation and collaboration with multiple stakeholders that can significantly contribute towards the improvement of the application.

3.5. Data Security and Privacy Concerns

Concerns related to Data Security and Privacy of the users has been identified as a matter of critical importance. The majority of the experts opined that the exposure/misplacement/ loss/

access/misuse of critical data to third party can act as a breach of data policy mandate set up by government and can further lead to violation of right to privacy. The Human rights expert stated that these issues can lead to stigmatization and discrimination of infected people. The legal expert also briefed about the loopholes in the privacy aspect of data collection and its implications like hate and violence. The privacy expert mentioned that *"multiple data points lead to 'under the skin' surveillance"* approach which is not healthy for functioning of the state. The computer software expert also remarked that "*...multiple data points of the app increases the privacy breach for the users. It can lead to excessive collection and use of sensitive personal data"*. Therefore, multiple data points increase the vulnerability of this mobile application. This aspect was agreed upon by majority of the experts, drawing attention to the critical information inputs that the App is taking more data than required and increasing the chances of data security and privacy violations. The human rights expert mentioned that *"It collects data on self assessment of COVID-19 symptoms and shows users the number of people having symptoms and tested positive in a radius of our own neighbourhood. It also sends alerts when a new person near our house tests positive or the user was in proximity of the person tested positive previously. In current times, anyone with the positive test reports be easily found in this much of radius"*. There have been reports of stigma, discrimination and violence against infected suspects at the community level in the country on the basis of the notifications by the app**.**

3.6. Worker's rights with respect to usage of the Aarogya Setu App

The aspect of Worker's rights with respect to usage of the Aarogya Setu app was acknowledged by all experts as being an important factor during critical times like lockdowns and the provisions of the same were not followed by authorities in ensuring the safeguarding of these rights, leading to stigmatization of the infected workers and their contacts resulting in incidents of violence, harassment, shaming and defamation due to leakages in the data related to their exposures and status of infection. The privacy expert explicitly mentioned that this app is like a 'privacy minefield' as even the worker's rights are being compromised through it and it does not adhere to principles of minimization, strict purpose limitation, transparency, and accountability

The human rights expert cited the individual example of delivery workers of *Zomato* Food delivering company *"Zomato made a decision to make it mandatory for its 'delivery partners' to use Aarogya Setu….at that time when app violates their autonomy and constitutional right to privacy which opened a door of discrimination towards Zomato valet, if they don't want to use the app or they will lose their job or get hate speeches from the customers if they will be going for home to home delivery of food without this app."* This instance shows the exploitation of workers in the absence of strict legal course of action in safeguarding of worker's rights.

3.7. Policy perspectives

The policy perspectives of the Aarogya Setu are centered much on the Personal Data Protection Bill 2019 (PDP 2019) which is still under consideration under a joint parliamentary committee. The technical experts mentioned how the Bill contains a number of provisions which seeks to

protect and uphold the privacy of data subjects. They law expert highlighted the section of exemptions being a cause of worry in the Bill and how it has little relevance with respect to any major changes in the Aarogya Setu. The cyber security expert mentioned that PDP Bill has had influence on the design and further development of the application and it still follows what is mentioned there. The privacy expert mentioned that PDP Bill has not secured the data but helped the government to take the data.

The privacy expert mentioned that PDP Bill hasn't secured the data but helped the government to claim the data. He further stated *"The Aarogya Setu app is a privacy minefield…."* Further, the technical expert also remarked that mobile app development should strictly follow the general data protection and privacy guidelines of the PDP Bill so that there is no violation of its clauses occur in the future. The expert further mentioned that *"As per the personal data protection bill, it seeks to provide the protection of personal data of the individuals, creates a framework for processing such personal data, and establishes a Data Protection Authority for the purpose… Yes, the presence of data security policy would have strengthened the data security aspects of the app"*

The app collects sensitive personal data than required and is not in alignment with the principle of data minimization and has been reported to be hacked multiple times by various ethical hackers.

3.8. Legal perspectives, implications and information related to Grievance Redressal Mechanisms

The legal perspectives, implications and information related to Grievance Redressal Mechanisms were answered best by the experts as per their individual knowledge on the legal frameworks. The legal expert mentioned that *"While the app was always touted to be voluntary, the police in many areas have been forcing people to download it. This is not permitted under the ambit of current law".* The expert further stated that *"Under the personal data protection act, only the Data protection officer can file a complaint to the Data Protection Authority related to the violation of data privacy, hence no individuals who's privacy has been violated can directly file a case against the government".* The privacy expert mentioned that *"the government is placed differently from a private entity in terms of how directly it can affect our rights as citizens. As a result, the State's actions could easily have grave impacts on citizens' autonomy in the long-term".* This calls for an urgent need to have a common legal framework for all mandated by the legislature and executives. The technical expert also noted that the installation of the Aarogya Setu App is a "voluntary decision, although forced in some cases under the provisions of the IT Act and the PDP bill. Two experts expressed needs of Intermediary Liability to ensure data security in the legal framework while one commented on the ambiguity of the current legal framework and grievance redressal mechanism as the users are unaware of the point of contacts to reach out to, in case of violation of their data privacy and security.

Table 6. Themes and Codes extracted from experts' opinions

S. No.	Themes	Responses
1.	Disclosures related to Privacy Policy	• Purposeful use of users' data • Third-party sharing of data • Uncertainty in ownership of data • Huge gap in Privacy Policy • Non inclusion of updates in Privacy Policy • Breach of right to privacy • Lack of notification to users in change in privacy policy
2.	Robustness and Security Aspects	• Linking of server with other government datasets • Threat of mass surveillance • No provision of deleting the account • No privacy by design to validate the architecture
3.	Lifespan/ removal of the application as mandated by the government	• Purpose limitation • Lack of clarification of the methods of erasure • Good decision to put a lifespan on usage • Implementation challenges • Need of transparent auditing • Lack of norms for monitoring
4.	Availability of Codes in the public domain	• Disclosure • Need of involvement of multiple stakeholder • Detection of Bugs • Assessment of Robustness • Open sourcing of codes • Transparency of codes
5.	Data Security and Privacy Concerns	• Breach of sensitive personal information • Breach of data • Violation of Right to Privacy • Perpetuation of stigmatization • Discrimination • Users' data at risk • Multiple data points • Hate mongering and violence • Issue of Transparency and Accountability
6.	Worker's Rights	• Stigmatization of Workers • Inaccurate prediction and analysis • Lack of mechanism to monitor leakage

		• Forced installation • Violation of rights • Compromise of Workers' autonomy • Deprivation of Worker's Privacy • Lack of adherence to principles of minimization
7.	Policy perspectives	• Weak Data Protection Bill • Weak implementation of Policy
8.	Legal Perspectives, implications and information related to Grievance Redressal Mechanisms	• Lack of clarity on answerability • Weak legal framework • Lack of grievance redressal mechanism

Discussions

There is a growing consensus towards use of a combination of medical and technological tools to scale up the response to a level to outpace the spread of COVID-19. However, there are issues around the wide implementation and adoption of these tools due to concerns around protection of patients' privacy and confidentiality and their data security and civil liberties (12).

A rapid evidence review conducted on digital contact tracing, symptom tracking apps and immunity certification reported an absence of evidence to support the immediate deployment of these technologies in response to COVID-19. The review recommended demonstration of technical capabilities and addressing of practical issues including legal tests for successful implementation of these technologies. It also recommended mitigation of social risks and protection against exacerbating inequalities and vulnerabilities (13).

A white paper reviewing the trade-offs of implementation of digital contact tracing reported that these technologies can achieve the goals of public participation, smart testing and effective resource utilization only if they can assure complete control of an individual over disclosure and utilization of data along with protection of their individual rights (12).

Another paper on privacy considerations and related trade-offs around contact tracing COVID-19 mobile applications commented that there are always tendency of trade-off between the privacy of the patients and the privacy of other users in these tracing apps. However, it is possible to achieve increased privacy through investment in additional computational resources and involvement of key stake holders in the development and up-gradation of the application (14).

The MIT technical review on COVID tracing tracker apps by MIT reported that Aarogya Setu met 2 out of 5 criteria for transparency and other data security parameters (7). There are some security issues reported by the analyzers and scanners after the publication of the source code of Aarogya Setu mobile application in public domain. The Aarogya Setu team provided some responses in this context as mentioned in Table 7 (15).

Table 7. Response on the technical issues by Aarogya Setu team

S.No.	Technical Issue	Clarification by Aarogya Setu team
1.	Missing Google Play Services Updated Security Provider	Issue mitigated through in-built mechanism by Google Play Services
2.	Missing component permission	Can't be invoked externally; no threat
3.	Unnecessary permission	Permissions are required for proper functioning of the app.
4.	Weak encryption	Data stored locally is anonymized and does not disclose user's identity
5.	Insecure shared preferences	Encryption of data stored in shared preferences
6.	Storage of encryption key in shared preferences	No storage of sensitive data in shared preferences
7.	Enabling of Java script	Can be invoked by owner
8.	Non encryption of URL endpoints	Does not lead to any security issue
9.	Cryptographic Vulnerability	Does not expose any sensitive data, possible misuse is very less.
10.	Code Obfuscation	Use of standard encryption and decryption method
11.	Modification of App using Debugging to load external content	Secure
12.	Disabled SSL CA validation	False Positive
13.	External Data in Raw SQL queries	No SQL injection vulnerability exists in database.
14.	Improper Error Handling	No disclosure of sensitive information in errors

15.	Bypassing of Terms and Conditions	Does not pose any security threat.
16.	Enabling of Multiple HTTP methods	Does not disclose any sensitive information.
17.	Bypassing of root detection of App	Not specific to Aarogya Setu.

Considering the gravity of the issue, a joint statement was issued by networks of organizations of public health advocates, experts in digital privacy, science and technology policy advocates and other stakeholders demanded following to address the technical, legal, ethical and implementation concerns of Aarogya Setu application (16). The recommendations are provided in this statement under following domains:

1. Proportionality: The GoI must emphasize on issues related to design and architecture of this application, ensure transparency and effective public engagement and limit retention time and use of data. The best technological models and practices and interventions adopted by other democracies around the world should be used as a benchmark to assess this app. There should be a complete release of app specifications and source code of the current version of the app. There should be a commitment to permanently destroy the data and systems at the end of pandemic and it should not devolve in to permanent surveillance. Its use must not be made permanent by public and private actors.

2. Legality: There should be formulation of decentralized legal frameworks and legislation procedures to hold the responsible actors accountable for leakage/ inappropriate use of App data.

3. Necessity: The government must establish the actual technical effectiveness of the intervention along with a cost-benefit/ privacy impact analysis. The necessity should be reviewed continuously throughout the implementation of this intervention.

4. Oversight structures and processes: There should be creation of independent institutions for monitoring and evaluation of the programme. The involved agencies/ institutions should publish periodic reports and provide feedbacks for the improvement/ continuation/ discontinuation of the programme.

Limitations of the study: 1) The data security tool used to assess the security issues in the mobile application is an open source, basic tool. The analysis performed is a basic analysis. 2) The sample of respondents in the survey conducted to understand the users' perspective of the application is not a representative sample. Therefore, the findings cannot be generalized. 3) This is an exploratory study based on the published literature, open editorial articles and opinions of experts. Therefore, the quantification of the effects and impacts is not possible in this study.

Conclusion: The vulnerabilities in the mobile app and weak policy on the data security in India put sensitive data of millions of people at risk. There should be an in-depth analysis of the application by independent experts and should be fixed to protect the data and privacy of the users. A national data protection policy should be strengthened to further formalize this field. More independent review and analysis should be performed to evaluate the app on various aspects.

Disclaimer

The views and opinions expressed in this exploratory research are based on personal experiences and analysis of the content available in various forms of literature. The opinion does not represent any organization or institution.

Acknowledgement

We acknowledge the contribution of Mohammad Afzal Shadab, The University of Texas at Austin in mobile application security testing through ImmuniWeb ® Community Mobile App Security Test.

Funding

The study is not funded

Conflict of Interest

No conflict of interests

References:

1. WHO. COVID-19 Public Health Emergency of International Concern (PHEIC) Global research and innovation forum. World Heal Organ [Internet]. 2020;7. Available from: https://www.who.int/publications/m/item/covid-19-public-health-emergency-of-international-concern-(pheic)-global-research-and-innovation-forum%0Ahttps://www.who.int/publications/m/item/covid-19-public-health-emergency-of-international-concern-(pheic)-glob
2. World Health Organization (WHO). Coronavirus disease (COVID-19) Global epidemiological situation.
3. World Health Organization. Digital tools for COVID-19 contact tracing. 2020;(June):4.
4. Daniel B, Gillmor K. Principles for Technology-Assisted Contact-Tracing. 2020;
5. World Health Organization. Ethical considerations to guide the use of digital proximity trackin technologies for COVID-19 contact tracing. 2020;(May):6.
6. WHO. Contact tracing in the context of COVID-19. WHO Guidel [Internet]. 2020;2019(May, 10):1–7. Available from: https://www.who.int/publications-

detail/contact-tracing-in-the-context-of-covid-19

7. Patrick Howell O'Neill, Tate Ryan-Mosley BJ. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. | MIT Technology Review [Internet]. [cited 2020 Sep 23]. Available from: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

8. India G of. Aarogya Setu FAQs 1 Functional General [Internet]. [cited 2020 Sep 23]. Available from: https://web.swaraksha.gov.in/in/.

9. Of ME and IT. Aarogya Setu is now open source [Internet]. [cited 2020 Sep 23]. Available from: https://static.mygov.in/rest/s3fs-public/mygov_159050700051307401.pdf

10. Immuniweb. Mobile App Security Test | Test Security of Your Mobile Application [Internet]. [cited 2020 Sep 23]. Available from: https://www.immuniweb.com/mobile/

11. Stoyanov SR, Hides L, Kavanagh DJ, Wilson H. Development and Validation of the User Version of the Mobile Application Rating Scale (uMARS). JMIR mHealth uHealth [Internet]. 2016 Jun 10 [cited 2020 Sep 23];4(2):e72. Available from: /pmc/articles/PMC4920963/?report=abstract

12. Leibrand S, Kakade S, Latta S, Lewis D, Tessaro S, Weyl G, et al. Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks. 2020.

13. Institute AL. Exit through the App Store? Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf

14. Cho H, Ippolito D, Yu YW. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. 2020; Available from: http://arxiv.org/abs/2003.11511

15. India G of. Clarification on Aarogya Setu [Internet]. [cited 2020 Sep 23]. Available from: https://static.mygov.in/rest/s3fs-public/mygov_159056968451307401.pdf

16. Joint Statement on Aarogya Setu -Technical, legal, ethical and implementation concerns during COVID-19 - Kractivism [Internet]. [cited 2020 Sep 23]. Available from: https://kractivist.org/joint-statement-on-aarogya-setu-technical-legal-ethical-and-implementation-concerns-during-covid-19/