INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 5

2020

Aarogya Setu: Privacy in the Time of the Pandemic

MANIYA GOYAL[1] AND SALONI KHANDELWAL[2]

ABSTRACT

The global coronavirus pandemic has affected almost every part of the human domain around the globe. It has taken countless lives and changed livelihood of many. What came as a boon from the app for India was the excess need for the implementation of the Data Protection Bill. A lot of countries brought forth contract tracing app as a strategy to tackle the pandemic and following the footsteps India too brought such an app called "Aarogya Setu" meaning bridge to health. The app was brought under the National Disaster Management Act, 2005 which works as an umbrella clause for the government to take action in times of pandemic and national disasters. The paper discusses the legal framework behind the app and the loopholes surrounding the same. There have been various privacy concerns in relation to the app such as use of Bluetooth and GPS, liability clause, data breach to name a few which are further elaborated. Justice Srikrishna headed the committee to draft the Data Protection Bill, 2018. A critical viewpoint of Justice Srikrishna has also been discussed in the paper. Once the pandemic is over what will be the aftermath of the app?, whether the app is a result of an executive action or a legislative one?, is the app in consonance to the provisions of the IT Act and the Data Protection Bill?, are countries implementing a similar approach? Are some question which are addressed in the further segment of the paper. The paper ends with some conclusion and recommendation which can be brought forth thus instilling a trust factor in the citizens of the country.

I. INTRODUCTION

The British Mathematician, Clive Humby once famously said, "Data is the new oil." Metaphorically, he explained that data is a resource, just like oil. It is useless in its unrefined form but becomes of enormous value once it is refined. Similarly, a lot of information can be extracted from data just as energy can be extracted from oil.

The global coronavirus pandemic has ensured the destruction of the status quo in almost every domain of human activity. Th crisis picking up the pace and thus destroying countless lives and livelihoods, governments and technology companies are also busy chipping away at

[1] Author is a student at NMIMS, School Of Law, Mumbai, India.
[2] Author is a student at NMIMS, School Of Law, Mumbai, India.

 [ISSN 2581-5369]

privacy rights. The over-reliance on data and the blind belief in one-stop technological solutions have prepared the stage for a proliferation of surveillance technologies making a springboard entry during the crisis. India too have joined the race and developed the contact tracing app called Aarogya Setu.

The app Aarogya Setu means "bridge to health" in Sanskrit. This contact tracing app is developed by the National Informatics Centre of the Indian Government which let one knows of our interaction with someone who could have tested positive for Covid-19 through a Bluetooth and Location generated the social graph. Previously, it was used known by the name of "Corona Kavach" app which was upgraded to the present form.

The paper deals with various angles related to the app, beginning with the legal framework surrounding the app. The app was brought under the National Disaster Management Act, 2005 by constituting a special executive committee for development of the app. The various controversies regarding the law behind the app and the constitutional bargain has been discussed further in the paper.

The app deals with various privacy concerns and each of the concern has been dealt in detail in the paper. The major drawback for India regarding the introduction of a contact tracing app is the lack of personal data protection bill and issues regarding the same have also been discussed. Justice BN Srikrishna, who chair the committee for drafting of the Data Protection Bill also termed the mandatory use of the app as "utterly illegal" and pointed that the app was not brought under a proper law and therefore any protocol, guideline regarding the same is illegal.

Aftermath of the pandemic in relation to the Aarogya Setu App has been discussed as to what will happen with the app and the data collected once the pandemic is over. Such an app is not only introduced in India but in other countries as well. The important aspect when discussing a global pandemic it is necessary to discuss the international perspective regarding the contact tracing app and the data privacy laws. Therefore, an international scenario regarding such apps and the viewpoint of international experts and analysts regarding the Aarogya Setu App has also been discussed. In the end the paper concludes with some recommendations and suggestions regarding the contact tracing app and what could be the dos and don'ts in relation to the app.

II. LEGAL FRAMEWORK

Aarogya Setu, the official Covid-19 tracking app of the Union government was launched in April for both Android and iOS users. The app was developed by the National Informatics

 [ISSN 2581-5369]

Centre, which comes under the Ministry of Electronics and IT.[3] There does not appear to be any particular legal framework that governs the app apart from a privacy policy and terms of service that have been updated a number of times.[4]

The legal framework for the government's pandemic management strategy has been the National Disaster Management Act, 2005 (NDMA)[5],which has an umbrella clause permitting the issuance of guidelines and directions aimed at addressing disasters.[6] Section10 of the NDMA[7] authorises the central authority to issue guidelines and directions to the several state governments with respect to addressing disasters.[8]

Data collected and processed by Aarogya Setu is governed by the app's privacy policy and a 'protocol' released on May 11, 2020 by an Empowered Group constituted under the NDMA.[9] Initially the app was released for voluntary use but subsequently made mandatory for all public and private employees under Guideline 15 of Annexure 1 released in May. Further, the highlight is that NDMA overrides other legislations.

According to the app's terms and conditions, the user "agrees and acknowledges that the Government of India will not be liable for…any unauthorized access to your information or modification thereof." This also goes against the provisions of the IT Act and the proposed Personal Data Protection Bill as the app service provider would fall under the definition of an intermediary and should be obligated to ensure the security of the data collected and should be liable for loss of it under the intermediary guidelines.

Various concerns were raised by legal experts upon the authority of the executive group established under the NDMA to issue directions which potentially impede upon the fundamental right to privacy of citizens, without a specific and explicit parliamentary legislation on the subject. It can be understood from Part III of the Constitution that before discussing that whether a right is violated or not, it is essential that there must exist a law

[3]*Aarogya Setu App: COVID-19 Tracker Launched to Alert You and Keep You Safe*, NATIONAL INFORMATICS CENTRE, MINISTRY OF ELECTRONICS & IT, https://perma.cc/44NU-YERK.
[4]Aditi Agrawal, *Aarogya Setu Updates Privacy Policy, Terms of Service: Reverse Engineering Not Banned, but Function Creep Now Legitimized*, MEDIANAMA (May 24, 2020), https://www.medianama.com/2020/05/223-aarogya-setu-privacy-policy-terms-of-service-update/.
[5]National Disaster Management Act, 2005.
[6]Gautam Bhatia, *The Mandatory Imposition of the Aarogya Setu App Has No Legal or Constitutional Basis*,THE WIRE (May 4, 2020), https://thewire.in/law/the-mandatory-imposition-of-the-aarogya-setu-app-has-no-legal-or-constitutional-basis.
[7]National Disaster Management Act Section 10, (2005).
[8]Gautam Bhatia, *Coronavirus and the Constitution – III: The Curfew and the Quarantine*, WORDPRESS (Mar.27, 2020), https://indconlawphil.wordpress.com/2020/03/27/coronavirus-and-the-constitution-iii-the-curfew-and-the-quarantine/.
[9]Harsh Walia and Abhinav Chandan, *Aarogya Setu: Why govt must take more steps to ease data privacy, liability concerns*, VCCIRCLE (June 12, 2020), https://www.vccircle.com/aarogya-setu-why-govt-must-take-more-steps-to-ease-data-privacy-liability-concerns/.

 [ISSN 2581-5369]

which authorises it. Any such law has to be specific and explicit with respect to the rights that it seeks to infringe, the bases of infringement, the procedural safeguards that it establishes, and so on.[10]

The NDMA cannot be said to be such a law as it absolutely imposes no limitations upon the government to limit or infringe rights of the citizens which in the present case is the right to privacy. The law is generic enough so as to permit just about *any* decree that the executive believes is required to tackle the disaster.

The NDMA is just one piece of legislation which acts as one single umbrella law that stipulates that "the government may do anything that it believes is reasonable to achieve the public interest" , and do away with any further need for law making *in toto*. This, however, is the very definition of rule by executive, instead of the rule by and of law.

The requirement of specific legislation is not a mere procedural quibble, but a crucial constitutional point, which raises one important issue of separation of power. If the government wants to introduce an app which is said to violate the privacy of the citizens then it atleast need to be authorized by the citizens' elected representatives in the parliament. Blithely mandating Aarogya Setu in one sentence through an executive decree tears the constitutional architecture to shreds.

III. PRIVACY CONCERNS SURROUNDING THE AAROGYA SETU APP

Arnab Kumar, the head of the project had stated that the app was built to the standards of the draft data privacy bill, which is currently in the country's parliament, and "access to the data it collects is strictly controlled.[11] Such data "is encrypted using state-of-the-art technology and stays secure on the phone till it is needed for facilitating medical intervention.[12] However, when the app was first introduced and even now, political leaders, experts and human rights organizations have expressed several criticisms and highlighted a number of privacy concerns some of which are as follows:

(A) Legality of making the app mandatory

Experts have noted that India is currently the only democratic nation in the world that had made its coronavirus tracking app mandatory for a significant portion of its population.[13] Vrinda

[10] Bhatia, *supra* note 4.
[11] *Aarogya Setu: Lack of Data Privacy Laws, Transparent Policies Make App Worrisome, Say MIT Researchers*, FIRST POST (May 11, 2020, 13:08 PM), https://www.firstpost.com/tech/news-analysis/aarogya-setu-the-mandatory-contact-tracing-app-of-india-gets-reviewed-by-mit-university-here-is-what-they-think-8354661.html
[12] *Id.*
[13] Patrick Howell O'Neill, *India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy*, MIT TECHNOLOGY REVIEW (May 7, 2020), https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-

Bhandari of the Internet Freedom Foundation in one of its interview with *The Quint* have said that the app should have been brought under the proper authority of law and should have satisfied the necessity and proportionality test for the violation of privacy.[14] A law under the Disaster Management Act was not enough.

The Internet Freedom Foundation pointed out: "Critically, India lacks a comprehensive data protection law, outdated surveillance and interception laws, or any meaningful proposals for meaningful reform.[15] In domains like disaster relief most apps which are purported as 'contact tracing' technologies, they often devolve into systems of movement control and lockdown enforcement.

May 7, the *MIT Technology Review* highlighted a number of similar concerns including the absence of a national data protection law.[16] This has raised the concern that the use of the app and its data collection has an "ambiguous legal basis."[17]

PMO office have made the use of the app mandatory for all private and public sector employees. Food delivery start-ups like Zomato and Swiggy have also made the app mandatory for all its staff.

(B) Using Bluetooth and GPS

Aarogya Setu uses the phone's Bluetooth and GPS which "stores both location data and requires constant access to the phone's Bluetooth," to track the user's movement, making it more invasive than other such apps.[18]

On May 11, 2020 the Ministry of Electronics and IT published a notification the Aarogya Setu Data Access and Knowledge Sharing Protocol.[19]This allowed it to collect demographic, contact data, self-assessment and location data of persons infected by the coronavirus or those who come in contact with the infected person.

According to *Livemint,* other apps collect just one data point which is later replaced with a

setu-covid-app-mandatory/.

[14]Vakasha Sachdev, *Is it mandatory to download the Govt's Aarogya Setu App?,* THE QUINT (Apr. 29, 2020, 14:43 PM),https://www.thequint.com/coronavirus/faq/faq-pm-modi-asked-to-download-aarogya-setu-coronavirus-app-but-is-it-mandatory.

[15]*Is Aarogya Setu privacy-first? Nope, but it could be-- If the government wanted. #SaveOurPrivacy,* INTERNET FREEDOM FOUNDATION, https://internetfreedom.in/is-aarogya-setu-privacy-first-nope-but-it-could-be-if-the-government-wanted/.

[16]O'Neill, *supra* note 11.

[17]Tripti Dhar, *Aarogya Setu – Carrying Your Privacy in Your Hands?*, PRIVSEC REPORT (May 29, 2020), https://gdpr.report/news/2020/05/29/aarogya-setu-carrying-your-privacy-in-your-hands/.

[18]Andrew Clarance, *Aarogya Setu: Why India's Covid-19 Contact Tracing App Is Controversial*, BBC NEWS (May 15, 2020), https://www.bbc.com/news/world-asia-india-52659520.

[19]Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020, https://perma.cc/WPH6-S6CY.

scrubbed device identifier, but Aarogya Setu collects multiple data points for personal and sensitive personal information which increases privacy risks.[20]

While the government says the data is anonymised and scrubbed of personally identifiable detail, the Software Freedom Law Centre pointed to a vague clause in the privacy policy which could "lead to excessive collection and use of sensitive personal data."

While the app also does not specify which government departments will have access to the database, the new protocol says data can be shared with the Indian government, and all the agencies that are granted access to the data must use it only for the purpose for which it has been shared and delete it after 180 days. There is also concern that health surveillance, which is "a necessity in a pandemic," "can soon evolve into mass surveillance."[21]

The government has published two ironical statements. In one of the interview with *The Guardian,* Abhishek Singh, one of the developers of the app had said that the data collected by the app will only be used for medical purposes and will not be shared with any third party.[22] In the meantime a new protocol of the government was notified stating that the personal data will be anonymised when it is shared with a third party.[23] These statements itself shows the lack of clarity among the developers and the government thereby putting privacy of the citizens at risk.

IFF has also pointed out that the government says the Terms of Service and the Privacy Policy of the app do not fall under the category of anonymised data sets. IIF in its working paper also stated that government cannot merely say that something is anonymised without ensuring the same to its citizens.[24] Minimum standards of transparency is a must where people' personal information is at the hands of government so termed as anonymous datasets.

(C) It's not open source

Until recently, Aarogya Setu app was not open source, it means that the code for the app is not available to the public despite government's policy. Baptiste Robert, ethical hacker and cyber security researcher, who famously goes by the name Elliot Alderson has said that if the

[20]Bloomberg, *Aarogya Setu: Govt's coronavirus tracker app gets 5 crore users in 13 days,* LIVEMINT (Apr 16, 2020), https://www.livemint.com/news/india/aarogya-setu-govt-s-coronavirus-tracker-app-gets-5-crore-users-in-13-days-11587021032271.html.
[21]Anand Venkatanarayanan, Op-ed, *Covid-19: How the Aarogya Setu App Handles Your Data,* BLOOMBERGQUINT (Apr. 17, 2020, 12:46 PM), https://www.bloombergquint.com/coronavirus-outbreak/covid-19-how-the-aarogya-setu-app-handles-your-data.
[22]Hannah Ellis Peterson, *India's Covid-19 app fuels worries over authoritarianism and surveillance,* THE GUARDIAN (May 4, 2020), https://www.theguardian.com/world/2020/may/04/how-safe-is-it-really-privacy-fears-over-india-coronavirus-app.
[23]*Central government's response to the COVID-19 pandemic (May 11 – May 22, 2020),* PRS LEGISLATIVE RESEARCH, https://www.prsindia.org/theprsblog/central-government's-response-covid-19-pandemic-may-11-–-may-22-2020.
[24] *supra* note 13.

government force the citizens to install an app by the law, the bare minimum they can do is to open source its code. Since the app is not open source it flaws cannot be reviewed and corrected by third parties.[25]

Making the source code available enhances transparency and this also improves security as the code is open to community audit.[26] The app primarily collects personal data from user cell phones and these are an immense repository of personal data of users and sometimes, of a user's contacts and acquaintances. In this scenario, keeping the source code of such an app proprietary is not advisable.

Contrast this with Singapore's Trace Together app and the contact tracing app used by United Kingdom's National Health Services, were both open sourced.

On May 26, the Ministry of Electronics and IT announced that the software has been made open source for android version and was open for review and collaboration.[27] A few weeks later the iOS version was released.

(D) The lifespan of the app and its data systems

Initially, the data was deleted on a rolling basis, 60 days for sick individuals and 30 days for healthy and the personal information was to be removed from the server after 45 days. Later according to the new protocol of the government it was notified that the data will be permanently deleted after 180 days. Also, individuals can seek deletion of the data withing 30 days on request basis. Government protocol also allowed it to hold on to the data beyond 180 days if a specific recommendation is made by an empowered group on technology.[28]

The main loophole pointed out by the Internet Freedom Foundation and many experts was that there was no mechanism for the individuals to check whether or not the personal information is deleted and there is no means of transparently auditing what the app is doing in the backend. To avoid the repressive measure of the government individual are filling incorrect data and there is no means to verify it, thus the efficacy of the data is questionable.

The MIT Technology Review pointed out that there was no public sunset clause stating when the app will stop being mandatory.

---

[25] Neerad Pandharipande, *'Indian Govt Should Convince Public on Aarogya Setup's Efficacy rather than Forcing It on Them': Cybersecurity Expert Elliot Alderson Tells Firstpost*, FIRSTPOST (May 23, 2020, 15:06 PM), https://www.firstpost.com/india/indian-govt-should-convince-public-on-aarogya-setus-efficacy-rather-than-forcing-it-on-them-cybersecurity-expert-elliot-alderson-tells-firstpost-8400371.html.

[26] Clarance,supra note 16.

[27] Press Release, Ministry of Electronics & IT, Aarogya Setu Is Now Open Source (May 26, 2020, 20:18 PM), https://pib.gov.in/PressReleasePage.aspx?PRID=1626979.

[28] *supra* note 21.

The Guardian reported that, "Unlike in most other countries, there is no transparency on the limitations on the lifespan of database and no binding policy that it will not be repurposed after the pandemic."[29]

(E) Data breach

In a blog post on *Medium* on May 6, French ethical hacker Elliot Alderson, observed a number of security concerns and flaws with the app, including that it was "possible to modify the location of the app, which can enable one to identify how many people are unwell or infected even without being physically present in their vicinity."[30] It basically let one see if someone was sick at the PMO office or the Indian parliament. However, he stated that in a subsequent version of the app, the issue was 'fixed silently' by the developers.[31]

MIT researchers have also pointed out that the app lacked on the parameter of "data minimisation" which means that the app is collecting more than is required for the app to work. One recent report highlights certain examples of this "non- adherence to the principle of data minimization": Example: the personal information collected includes detail of the individual's profession, which has no direct relation with the effective use of the app, proximity data should be used as opposed to location tracking.[32]

India has a chequered history with data privacy with Aadhaar being the world's largest and the most controversial biometric based identity database.

(F) No liability

According to the app terms and conditions "the user agrees that the Government of India will not be held liable for any unauthorized access to your information and modification thereof". It means that the Government will not be held liable even if the personal information of the user is leaked. It also limits the government's liability if the app provides inaccurate information or shows false positives.

This also goes against the provisions of the IT Act and the proposed Personal Data Protection Bill as the app service provider would fall under the definition of an intermediary and (is) obligated to ensure the security of the data collected and (is) liable for loss of it under the intermediary guidelines.

[29] Peterson, *supra* note 20.
[30] Pandharipande, *supra note 23.*
[31] *Id.*
[32] Dhar, *supra note 15*

 [ISSN 2581-5369]

IV. CRITICAL ANALYSIS OF THE APP IN RELATION TO JUSTICE SRIKRISHNA AND THE DATA PROTECTION BILL

In August 2017, the Supreme Court of India held the right to privacy as a fundamental right. Still citizens suffers from the threat of data privacy since the government has no clear legislation on privacy to monitor data protection. A committee headed by Justice Srikrishna submitted a report in July, 2018 followed by a draft of the Data Protection Bill. The committee recommended several rights for the data principal (whose personal data is collected) from revoking consent granted for processing data, notifying a breach to having their incorrectly processed data rectified by the authorities. Despite there being a draft bill yet the there is a void in the legislation regarding privacy because the bill is yet not approved in the parliament.

The lack of personal data protection regulation gives the government powers of surveillance. The Information Technology Act, 2000, for instance, allows widespread communications interceptions by the government in the event of a security or national threat.[33] Given these powers of the state, the worry is that Aarogya Setu could become a citizen-surveillance tool.

A protocol was issued by the government for Aarogya Setu which set forth the principles for collecting and processing of data. The protocol is an order by the Empowered Group on Technology and Data Management set up by the National Executive of the Disaster Management Act.

Justice Srikrishna in relation to the protocol pointed that such an order is issued at the executive level and is not backed by Parliamentary legislation which holds more backing of law. As per Entry number 97 of the Seventh Schedule of the Constitution of India, a legislation on data collection and use would be covered only by the Union list, and thus, only the Parliament would have the power to legislate on such a subject.[34] In view of the same, the NEC cannot use the Disaster Management Act, 2005, to formulate guidelines on data collection and use. Therefore, such an action suffers from excessive delegated legislation "horizontally".[35]

Also, NDMA has no provision for the constitution of an empowered group, so therefore the law is in question behind the order. The provisions are vague in terms of the liability it creates, as to who should be held accountable in case of data breach. Justice Srikrishna also recommended the tracing of the app back to the Personal Data Protection through an appropriate amendment. The bill does have an enabling provisions which best suits the scenario

[33] The Information Technology Act, 2000.
[34] Constitution of India, Entry 97, Seventh Schedule (1950).
[35] Raghav Ahuja, *The curious case of parallel legislature in the regulation of Aarogya Setu,* MEDIANAMA (June 2, 2020), https://www.medianama.com/2020/06/223-aarogya-setu-parallel-legislature/.

 [ISSN 2581-5369]

of Covid 19 under Section 12 which allows collection and use of such data in exceptional circumstances even without consent. Despite being a legislative void, the government is collecting data under Section 10(2)(1) of NDMA which allows the government to formulate guidelines on any domain of law with no restrictions in the name of disaster management.[36]"

On May 1, the Ministry of Home Affairs, notified through the guidelines that Aarogya Setu App has been made mandatory for employees of private and public sector offices. It also asked local authorities to ensure 100% coverage of the app in containment zones. The guidelines were issued by the National Executive Committee set up under the National Disaster Management Act (NDMA), 2005. Justice Srikrishna termed the government's push of mandating the use of Aarogya Setu app "utterly illegal".

Justice Srikrishna said that the guidelines cannot be considered as having sufficient legal backing to make the use of Aarogya Setu mandatory. Both pieces of legislation i.e. the National Disaster Management Act and Epidemic Diseases Act are for a specific reason and the national executive committee cannot be considered as a statutory body.

V. AFTERMATH OF COVID 19

The Knowledge Sharing Protocol has a sunset clause of six months which means that the personal data will be deleted after this period. But it also has a provision to extend the period of the sunset clause. It needs to be noted that this sunset clause does not apply to the Aarogya Setu app and the app may be repurposed after the pandemic. Fears of a function creep are already manifesting with the Aarogya Setu development team's plans for integrating telemedicine, e-pharmacies and home diagnostics to the app in a separate section called Aarogya Setu Mitr.

NITI Aayog officials have said that the app will have no use after the pandemic, but it will lay the foundations for building the National Health Stack (NHS).[37]

A report from *The Ken* points out that the Aarogya Setu will be the starter app for the National Health Stack similar to how BHIM was for the Unified Payments Interface (UPI).[38] The NHS is a set of cloud services which maintain a national health electronic registry, a coverage and claims platform, a personal health records framework and an analytics platform that can be accessed through a set of APIs by third parties.

[36] National Disaster Management Act, Section 10(2)(1), (2005).
[37] NITI Aayog, http://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf.
[38] VCCIRCLE,https://the-ken.com/story/the-elite-vc-founder-club-riding-aarogya-setu-to-telemed domination/#comment-1149067.

It is recommended that since India still does not have a Personal Data Protection law it would be unwise to expand the scope of Aarogya Setu far beyond its original purpose of tracing COVID-19 patients. It is still unclear how the National Health Stack's consent platform will work and if there are enough safeguards for sensitive personal data including health records, prescriptions and discharge summaries. Moreover, India currently ranks number third in terms of COVID-19 positive cases at the time of writing this. Therefore, it becomes more crucial that Aarogya Setu fix its problems of exclusion for effective health monitoring rather than building more functions. There is a need for the government to demonstrate the effectiveness of the app to build trust between citizens and frontline health workers.

VI. A GLOBAL VIEWPOINT

India is not the first country to deploy technology for coronavirus contact tracing, there are other countries like China, US, Singapore, Hong Kong and various European countries have such apps. Many fear that in country like India with no meaningful anti-surveillance, privacy or data protection laws it will have a sinister implication.

Famous Indian author Arundhati Roy has stated that, "The coronavirus is a gift to authoritarian states including India". She also explained it with an analogy stating that pre-corona the country was sleepwalking into a surveillance state and now the country is panic-running into super-surveillance state.[39]

MIT Technology Review's Covid Tracing Tracker list 25 such kind of contact tracing apps and have found some of them going beyond what is needed. Example: China's Health Code System is one of it. It records a user's spending history in order to deter them from breaking quarantine, which in a way is invasive.[40]

MIT University has reviewed the *Aarogya Setu* app to understand how effective is the app, is it safe to use, and how it compares to other contact tracing apps that are being used in different parts of the world. The policy of the app suggest that the app is voluntary but later the app was made mandatory and thus India became the only democratic nation in the world to have such mandate. Another concern raised was the accessibility point, it was not clear as to get the access to the data. The policy of the app is not transparent and the icing on the cake is the lack of national data protection law. French ethical hacker Alderson presented the mandatory use of

[39] *supra* note 20.
[40] O'Neill, *supra* note 11.

such contact tracing app as a work of repression and not a success story.[41]

It is not like every country have flaws in their system for e.g.: in Singapore the TraceTogether app is only being used by its health minister to access data. It assures its citizens that the data will be used strictly for disease control and will not be shared with law enforcement agencies for enforcing lockdowns and quarantine.

VII. CONCLUSION/RECOMMENDATION

The paper discusses various aspects surrounding the Aarogya Setu App starting with the legal framework surrounding the app. An app brought with an intention to curb or somehow control the rising cases of Covid 19 was turned into a surveillance tool.

First recommendation in regards to the first aspect i.e. the legal framework surrounding the app is that the government should not delay more in bringing the data protection bill into enactment. A proper legislation might fill in all the voids and bring a sense of security in the minds of the citizens regarding their data.

In respect to the second aspect concerning the privacy issues in the app, enacting the Data Protection Bill would be the most advisable suggestion. If that is a far-fetched dream then a more transparent policy regarding the App would be of instant use.

Moving towards the aspect which discusses the aftermath of Covid 19. Government should make it clear to the public that there personal information is safe and secured and is getting deleted as told to them. Government should not focus on the future aspects of the data collected rather bring forth the Data Protection Bill and also assure to its citizens that data their information is not getting misused and their fundamental right to privacy is upheld.

Conclusively, the government should make every effort to win back the trust of the individuals in lieu of the chequered history of India regarding privacy of data. Without this discourse, the new world and the digital-age present the risk of becoming a glass-house, whose see-through walls would allow too much exposure to the light of ubiquitous surveillance and public scrutiny, thus, scorching our private-selves, and in doing so, would arrest and encumber the organic growth and development of the "inviolate personality," which requires shade and shelter in which to flourish.

*****

[41] *supra* note 18.

 [ISSN 2581-5369]