Nat. Volatiles & Essent. Oils, 2021; 8(6): 3310-3322

NVEO
Natural Volatiles &
Essential Oils

Is Contact Tracing Application An Eclipse On The Right To Privacy Of Sensitive Health Data: An Analysis Of The Aarogya Setu App

Akriti Kaushik[1] , Prof. Raj A. Varma[2]*

[1]LL.M. Student, Symbiosis Law School, Pune, Symbiosis International (Deemed University)

[2]Assistant Professor, Symbiosis Law School, Pune, Symbiosis International (Deemed University)

Abstract:

Every State today stands at a different footing under the global pandemic. With the help of artificial intelligence, many countries have successfully launched their own contact tracing application to understand the pattern of virus, its growth and later use this application for easing down the restrictions. The Government of India, too launched its own application - "Aarogya Setu." Since the day of its launch, till date, there has been constant criticism surrounding it. The lack of proper guidelines on data privacy and no statutory law backing it, the use of this application inevitably poses a big threat to the privacy rights of every registered user. The current application runs on machine learning and algorithms and profiles every user through constant surveillance. The government can, if need be, mandate the use of this application under "reasonable restrictions." The author thus tries to analyse the privacy rights of every individual who uses this application and if the guidelines on surveillance and contact tracing applications released by the World Health Organization are being complied with by the Indian government or not.

Keywords Artificial Intelligence, Data Privacy, Machine Learning, Surveillance, Reasonable Restriction.

Unlocking the "Reasonable Restrictions" in a State of health emergency

The world today is fighting a highly contagious pathogen termed- COVID-19. Spreading across the globe like wildfire, every country declared a national lockdown and restricted the international travel completely for public health and safety. India too decided for a complete lockdown on 23rd March 2020. For a country like India, with the second largest population, the challenges that stood in front of it were different and big. The lockdown was not really welcomed and was imposed onto the people. As the infection kept growing every day the Government of India decided to launch their contact tracing application- "Aarogya Setu", with the help of the Ministry of Electronics and Information Technology.

The objective behind developing this application was only to alert people about the risk once they

stepped out of the house[3]. The minute a person crossed paths with an infected person he would be profiled by the application and put under a category of high risk based on various aspects. The Prime Minister through his national address urged everyone to download the application and stay safe. In furtherance of the address, a government notification was released making the download of this application mandatory for government servants.

This new surveillance application faced continuous criticism and came under the radar of the privacy experts as well. Where the countries around the world checked twice before releasing any surveillance application like the United Kingdom to ensure that the rights of the citizens are not curtailed and released an advisory to check the measures before collecting any personal data and the surveillance applications being banned in Australia and New Zealand as were posing challenges to right to privacy, India took a major step of releasing the application. The application was looked at as a technologically advanced method for mass surveillance by the State. The privacy experts started questioning the working of the application and voiced their concerns. Where the application was used launched to protect the public and utilize the data for good governance, the picture turned out to be titled. The sudden transition from voluntary measure to being made mandatory was being labelled as a part of the same cloth as that of the Aadhaar which was initiated as a voluntary step but made mandatory by the government[4].The similarities between the two of being launched in void of any legal framework started to speak volumes about the threat that lies ahead for the government. With no strict guidelines on tracing, data collection, use of geographical locations, collecting sensitive information from every individual based on self-assessment manner had to raise serious concerns. While the world was fighting the pandemic, this new threat of being under continuous surveillance created more fear amongst all.

Is the State allowed to mandatory force the use of the contact tracing application or any application for the purpose of surveillance and restrict the free movement of its citizen or not became the debate of the hour? The minute this application is downloaded on a smart phone, it utilizes the geolocation and starts tracking every movement of the user. Though a user is free to move around, the application is putting the user under surveillance and the data collected by it is being stored with the government. One may be physically free to move around, the privacy rights of that individual are being curtailed as one may not wish to share all his details. To protect this right Article 19(1)(d) of the Constitution of India guarantees to every citizen a right to move freely throughout the territory of India[5]. The right to movement or locomotion means that a person is allowed to move freely or absolutely. The only time this right can be taken away is under "reasonable restriction." Now to check whether the restriction is reasonable or not it is important to see if it is in public interest at large or not[6]. The phrase "in the interest of the general public"

[3] Hindu N.D. (2020 May, 8). How does the aarogya setu app work? *The Hindu*, https://www.thehindu.com/news/national/how-does-the-aarogya-setu-app-work/article31532073.ece

[4] Aashiq P. (2020 May, 15). Government employees mandated to download Arogya Setu app in Srinagar, *The Hindu* https://www.thehindu.com/news/national/other-states/government-employees-mandated-to-download-arogya- setu-app-in-srinagar/article31595219.ece

[5] Singh M.P. V.N.Shuklas's Constitution of India (13 ed.). Eastern Book Company. 165

[6] *Id* at 3.

means the same thing as "in the public interest"[7] and will include public order, public health, morality, etc.[8]

So can the personal liberty and freedom be restricted if an order is passed by the government under the notion of "public health" To understand "personal liberty" one may then refer to the Supreme Court's take on the very first precedent on surveillance. The term "personal liberty" first came before the Supreme Court in the case of Kharak Singh Vs. State of U.P.[9] In the current case a history sheet was maintained by the U.P. Police of criminals who may turn into habitual offenders and thus were put under surveillance. The petitioner approached the court questioning his freedom of personal liberty as his every movement was recorded and at times police visited his house at night to check. The Supreme Court decided the matter relying upon the Universal Declaration of Human Rights (UDHR)[10]and stated that the personal liberty is very intricately linked to right to privacy and cannot be infringed. Surveillance is a threat to the personal liberty and life of any person and right to privacy is the most basic human right and hence is to be enjoyed by all.

Coming back to the question of mass surveillance and reasonable restrictions under times like this, one may also like to refer to the "Doctrine of colorable legislation". The doctrine explains that when a State wants to enact a legislature which is not allowed by the constitution or against is inconsistent to any provisions of the constitution, then it cannot go ahead and color the provisions to meet its suitability. So, in the present case where the government is not allowed mass surveillance, can it do so under the times of national health emergency?

The State needs to create a fine balance specifically in scenarios of health emergency where the sensitive health data of citizens might be at a great risk of unauthorized access. Thus, where the question is about national interest and public health, the reasonable restrictions should not be utilized by the State to meet its other purpose that destroy the whole essence of why restrictions are being imposed on the citizens.

No right is an absolute right:

The Epidemic Diseases Act, 1897 is the statutory law that lays down the conditions of imposing the restrictions in circumstances of emergency in wake of some infection, disease, or any other health related condition that can be a threat to human life. Where Article 19(1)(a)[11] imposes restrictions on freedom of speech and expression, the State is then given a free hand to curb the rights of the citizens by way of reasonable restrictions. Neither the Constitution of India defines the term "reasonable restrictions", nor it lays down a fine list what are the exact situations when the reasonableness be laid down to protect the general interest. The test may vary from one right to another which the law restricts.[12] However, what needs to be ensured is that these restrictions should not take away the basic rights of an individual. To test these restrictions, one should apply

[7] Kavalappara Kotharathil Kochuni V. State of Madras & Kerala, AIR 1960 SC 1104 (1960).

[8] *Supra* Note 3, pg 172, at 3.

[9] Kharak Singh V. State of U.P., AIR 1963 SC 1295 (1963).

[10] United Nations Declaration on Human Rights, Article 12, UNITED NATIONS, December 10, 1948.

[11] Constitution of India, art.19

[12] State of Madras V. V.G. Row, AIR 1952 SC 196 (1952).

the doctrine of proportionality[13]. Procedural requirements of natural justice flow from Article 19 of the Constitution. The "principles of natural justice" cannot be withered away with when considering reasonableness of the restrictions imposed. But the elaborate rules of natural justice maybe excluded expressly or by necessary implications where procedural provisions are made in the statute[14]. Where in a state of health emergency, the Epidemic Diseases Act allows the state to restrict the movement of people and quarantine them, can the State be allowed to go a step forward and put everyone under a continuous surveillance, well the answer to these questions depends on understanding the reasonable restrictions to maintain public health and order in the State.

Reasonable Restriction includes prohibition:

The word "restriction" can be understood as prohibition of movement. The State can establish a law that may deprive a person of his fundamental right, under an emergency[15]. The recent ordinance passed by the Epidemic Diseases Act, 1897, the State has allowed the police officials to investigate and prohibit movement of vehicles so that the outbreak of the disease could be stopped. The Act states that if there is a situation where the government is satisfied that there is a possibility of an outbreak of any dangerous epidemic disease orders maybe passed for temporary regulations to contain such epidemic and thus restrict movement and in furtherance of this also pass a notice amongst the public[16].

Reading the above stated provision into Article 21 of the Constitution, that provides right to life and personal liberty, one can state the restrictions imposed by way of an ordinance to protect larger interest, the restrictions can be termed as justified. Providing and ensuring safety of one's citizens has always been the biggest responsibility for any state. The problem arises when the any such law passed by the government fails the test of reasonability and the citizens feel that their rights are being curtailed and infringed upon. Thus, where restricting movement during nationwide lockdown passes the reasonability test, it poses a big question- whether the government has imposed such restrictions within its capability or how it outrightly surpassed the boundaries and taken a decision that is inconsistent with the constitution.

Foregoing the right to privacy under reasonable restriction:

The recent ordinance[17] passed by the President has raised many eyebrows as the right to privacy and personal liberty is put at stake when any such surveillance application is allowed to play with

[13] Singh M.P. V.N.Shuklas's Constitution of India (13 ed.). Eastern Book Company. 133

[14] Haradhan Saha V. State of W.B., (1973) 3 SCC 198 (1973).

[15] M.B.Cotton Assn. Ltd. V. Union of India, AIR 1954 SC 634 (1954).

[16] The Epidemics Diseases Act, 1897, https://indiacode.nic.in/bitstream/123456789/10469/1/the_epidemic_diseases_act%2C_1897.pdf

[17] Ministry of Health and Family Welfare, The Epidemic Diseases (Amendment) Ordinance, 2020, (2020 April, 22). https://www.prsindia.org/sites/default/files/bill_files/Ordinance%202020%20-

%20epidemic%20act%20.pdf

the citizens' rights. The reasonable restrictions can only be imposed when backed by a law[18]. In times of emergency, an ordinance is to be treated as a law for the time being and once the period is over, it can then be decided by the Parliament whether to convert it into a law or do away with it. So any such law or ordinance when enters the territory of "personal liberty" it needs to have a strong reason to curb it. The recently passed ordinance under the Epidemic Diseases Act, 1897 clearly permits the state to take away not only the liberty, but also compromises onto the privacy rights of individuals by detaining a person who wishes to travel. The ordinance thus provides a free hand to inspect any ship or vessel that arrives at any port or detain a person who intends to travel from port during the outbreak of the disease. Also, the central government is vested with the powers to inspect and regulate the movement of buses, trains, goods vehicle, aircrafts leaving or arriving any port, or aerodrome. Also, finally any person who initiates to travel at this time can be detained. Thus, the movement can be restricted in such times.[19]

Thus, where the State imposes reasonable restrictions for travel and other related services and starts to regulate every movement and may also detain any person who might not follow the lockdown guidelines introduced or act in contrary to the guidelines issued during the pandemic, or restricting the movement of any vehicle, good train, vessel, airplanes, or any other means of transport a strict civil and criminal punishment is imposed upon them. Article 19(1)(d) permits the freedom of movement, but Article 19(5) can put reasonable restriction on this free movement and curtail anyone from not complying with the lockdown guidelines issued in public interest.

The Supreme Court in the case of Maneka Gandhi[20] was faced with the same question on petitioner's right to personal liberty under Article 21. The petitioner's passport was impounded by the authorities and was barred consequently to travel abroad. Infringing with the right to life and personal liberty thus saw a new interpretation in this case. The restriction imposed by the law needs to be in line of reasonableness and not barge into a territory where it forced to be repealed.

So, where the current pandemic requires an individual to give up their rights of free movement, the State should ensure they are not constantly monitored around the clock.

Public health or Infringement of privacy: Maintaining a fine balance?

The constant debate around mass surveillance has reach a new peak in the world today. Where the State must shoulder the moral responsibility to keep the infection from spreading and contain it, it is forced to impose restrictions on all. The right to health and safety cannot be neglected by any State. The challenge that then arises is that- how will the state maintain the fine balance between the citizens' right to health and treatment with the other fundamental rights such as right to privacy, right to personal liberty and right to free movement.

India today, has the second largest population. With the help of the World Health Organization (WHO) guidelines on surveillance[21], India took a major step towards protecting its citizens from the

[18] *Supra* Note 7, at 3.

[19] *Supra* Note 12, at 4.

[20] Maneka Gandhi V. Union of India, (1978) 1 SCC 248 (1978).

[21] WHO, WHO guidance for surveillance during an influenza pandemic 2, United Nations (2017), https://www.who.int/influenza/preparedness/pandemic/WHO_Guidance_for_surveillance_during_an_influenza_pandemic_082017.pdf

global pandemic. The recently launched contact tracing application Aarogya Setu started to be seen as a helping hand for the State. The application based on artificial intelligence, helps to track one from the nearest Covid-19 patient based on geographical location and Bluetooth connection. It also provides the option for self-assessment and in case one feels they might have the infection, to call the helpline and receive medical aid. Where it makes receiving the medical aid easily what one skips here is the continuous collection of personal data from the user. The other services being provided through this application includes information on nearest laboratories for testing, inter-state travel passes, an inter-district pass as well. This tracking application has been developed by the efforts of the National Informatics Centre (NIC) and comes under the Ministry of Information and Technology.

The National Informatics Centre plays a significant role in delivering citizen centric e- services[22]. While the application helps one track how far they are from the next patient running in 500m, to 1Km to up to 10 Kms of radius. The contact tracing application has posed several privacy questions amongst all. It thus becomes crucial for the State to ensure that the application clearly states out its objective, reason for collection of data, for how long it will save the data, how will it protect the sensitive health information it collects from its users. The current use of such tracking devices has also been discussed at international level. “Some restrictions on people’s rights may be justifiable during a public health emergency, but people are being asked to sacrifice their privacy and turn over personal data for use by untested technologies,” as said Deborah Brown, senior digital rights researcher at Human Rights Watch[23]”. The application states that till date[24]about 13.38 crore citizens of India is using it.

The application utilizes artificial intelligence to assess a person based on the information it is fed. The algorithms then profile the user under one of the three zones- where red specifies one as a carrier of the infection, the orange zone assess one as to have come in close contact of someone who has been traced down as carrying the infection and finally, the green which states that the person is safe. Based on this profiling of an individual, the application goes a step further and states the next helpful steps in protecting oneself from falling a prey to the infection. The collection of such sensitive information from millions of users calls for a data protection regime, as the theft of any of this data could cause a major problem for India.

Protecting the Private health Data:

As Aarogya Setu has been asked to mandatorily be installed in mobile phones of millions of users, the responsibility of ensuring the data safety and privacy rights of these citizens cannot be denied by the State. Placing the Hohfeldian theory in the current scenario, where there are rights, there is

---

[22] National Informatics Centre, NIC Services- Our Core Services Towards a Digital Nation, Government Of India, https://www.nic.in/services-main-page/

[23] The Human Rights Watch, Covid-19 Apps Pose Serious Human Rights Risks -Recommendations for Governments Considering Technology in Addressing Pandemic, United Nations, (2020 May, 13), https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks(

[24] As on 25.06.2020, the number reflected on the Aarogya Setu app states that 13.38 crore users have been registered on the application.

duty[25]. While the citizens have a right to not be put under surveillance or be monitored or tracked for every minute one steps out of the house, the correlating duty upon the State is to ensure that the contact tracing application does not monitor them. The doctrine of colorable legislation also clarifies that "when one thing is not allowed directly, it cannot be done indirectly[26]." The government should therefore be vigilant that one cannot put others under constant surveillance where the Constitution restricts the same. The reasonable restrictions as discussed above allows something to be done only when it is not unconstitutional. Then does this application that is collecting information needs some regulation or guidelines to keep abide by so that the balance of rights is maintained. The State can govern peacefully while the rights of its citizens are intact. The constant answer thus everyone seeks here is, if regulated by guidelines how is the application to run and ensure data privacy in the healthcare sector where the sensitive health information stays vulnerable. What rights are dissolved and severed in a condition of state emergency and public health of a citizen who volunteers to. While the theory of no right can ever be an absolute in its nature and all have some restrictions and how it has been supported in the privacy judgement[27], it still becomes essential to discuss can an application like Aarogya Setu, that collects sensitive health data of every citizen in India, be allowed to profile a person. While the Government of India makes it mandatory to install this application, that allows surveillance as it keeps tracking the geographical location to alert one from the nearest Covid-19 patient can it be stated that a state of surveillance has been created and the government is enforcing a mandatory check on every citizen. If the State continues to take a positive stand on the current situation with a stronger argument that the application does not infringe the privacy rights of a person, one can be only assured if the application has the "do not track policy" inherited in the application[28].

Where every contact tracing application evades the privacy in one way or the other, what can protect the privacy rights of its users is only a secure and proper protection of information being done by the privacy policy. Thus, the answer to if privacy rights are protected or not one will have to read between the terms of the privacy policy of the application and the protocol governing the application.

Understanding the Aarogya Setu Protocol, 2020:

The application is being governed by the "Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020[29]." To control the pandemic and owing a duty towards the citizens the Central government launched the application while the States were to decide the mandatory use of application or not. Where some states accepted the Central Government's decision to make it mandatory some refused. The current Protocol is to remain in force for a period 6 months and then be reviewed again. This protocol deals with guidelines on which the collection of data is done

[25] Lazarev N. (2005) Hohfeld's Analysis of Rights: An Essential Approach to a Conceptual and Practical Understanding of the Nature of Rights, MurUEJL 9

[26] Gahrana G.K. (1964) *The Indian Journal of Political Science*, 25 (2), 27-37.

[27] Justice K.S.Puttaswamy (Retd.) and Anr V. Union Of India, (2017) 10 SCC 1 (2017).

[28] Privacy Policies. (2019 December, 30). Your Privacy Policy Must Include a "Do Not Track" (DNT) Clause, https://www.privacypolicies.com/blog/privacy-policy-dnt-do-not-track/

[29] *Supra* Note 11, at 4.

by the app and further clarifies the concerns regarding data safety.

The WHO guidelines suggest that the person giving his information should always consent to freely share his personal sensitive information with anyone after an informed consent is obtained. This means any person consenting to share his private data can choose whether to share his details. The minute one consents to share their data, they should be made aware of the purpose behind this collection of data, how it will be stored, processed, will it be shared with some third entity or not and finally how it will be deleted. Thus, the purpose behind this collection of data should always be made available to the consenting party. Under the protocol for Aarogya Setu the purpose should thus be limited to only know if someone caught the infection or not and no extra information should be demanded under the principle of data minimization.

The next important clause under the protocol is the time period for which the data will be stored. The protocol states that the data collected shall not be retained for a period than necessary to serve the original purpose of its collection and thus will not extend beyond 180 days. The data will then be deleted permanently. The application also collects demographic data i.e., location details, on this the protocol states that data will be deleted as soon as a request is made and if no such request is made it will be deleted maximum by 30 days from such request initiated[30]." The protocol also provides for the penalty clauses that states that any violation of the directions of the Protocol imposes on authorities may lead to penalties as per section 51 to 60 of the Disaster Management Act, 2005 and any other legal provisions as may be applicable. Where the protocol justifies under the principles about auditing the reports of the research colleges with whom the data might be shared to ensure privacy. The obligations stated out for the entities for with whom the data has been shared the Protocol states out in simple language the time period for retention of data, when will it be deleted permanently and what duty of care lies.

The Protocol emphasize upon restricting the processing of data only for the purposes it has been collected for and not to go beyond that. Any Ministry or government department should strictly adhere to these provisions. The data retention time period should at no cost be exceeded. Once the period of 180 days has lapsed, the data should be deleted permanently[31].

The other important feature to ensure privacy of the data there is always a need to have technical safeguards as well in place. The Protocol persists for anonymization and states that hard anonymization shall be used when soring the data. The Protocol explains the term "Hard anonymization" which means a series of technical processes are put in place which ensures that any individual information becomes incapable of being identified. The Protocol further clarifies that this anonymization shall be done in accordance with anonymization 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[32].

Thus, as we read the privacy Protocol for Aarogya Setu, one can say that the where the

[30] *Supra* Note 22, at 10.

[31] *Supra* Note 11, at 4.

[32] *Supra* Note 24, at 10.

government is trying to take several measures to protect the sensitive information shared by the users trusting the application however it can only be guaranteed if this protocol meets the privacy policy on which the application works.

Decoding the privacy policy of Aarogya Setu:

The current application has been launched by the central government with the help of the Ministry of Electronics and Information Technology. The server of the application registers a user on downloading the application onto their phone. Once downloaded, the application asks a person to keep their mobile phone's Bluetooth and location on for 120 seconds. Once done, the next step is to assess oneself based on questions that ranges from asking about health conditions. The application on registration collects various sensitive information like name, age, any past travel history, any previous medical history of lung infection, or heart related disease and once answering these questions, the application profiles the user in one zone out of the three. If one tests to be unfit the user is reached out by the Government of India helpline number and a healthcare personnel will contact and/or inform such registered users. The risk is analysed based on a user coming in contact with someone in past 30 days who might have a risk of being infected. Based on a similar pattern, a user will be notified if, because of having come in contact with any persons who has tested positive for COVID-19, might be at a risk of being infected. The application thus profiles one based on certain factors[33].

Looking at the service provided by Aarogya Setu app prima facie, one can see how the data collection starts the minute one downloads the application onto their phone. While it asks for permission to keep the location and Bluetooth on the entire time to track one cannot ignore the other risks that can occur simply having the Bluetooth being turned on when in public. Where the current application has been constantly being compared to the Contact tracing application of Singapore which does not use the GPS location to trace one, the Government tries to answer this question stating in the FAQs available in the application that the India is a diverse country with huge population and the same is required to be done technically. The present answer still does not qualify for a proper reasoning as to why can a similar application be launched for the Indian citizens as well.

Requirement Policy:

Moving forward, the privacy policy mentions the requirement for use in its policy. This part discusses consent and acknowledgement of downloading the application and giving the consent for it to use the location and Bluetooth to further provide its service. It mentions that in case one switches off or puts the mobile device on airplane mode the application may not give out or capture all necessary information that is required for completeness and accuracy of the Services[34].

Use:

The application states that the user consents to provide the required health information in good faith and will not provide false or misleading information about themselves or the symptoms regarding the infection status. The intention of using this application should only be to protect and

[33] Ministry of Health and Family Welfare, *Aarogya Setu*- Privacy Policy, Government Of India, https://static1.swaraksha.gov.in/privacy/

[34] *Supra* Note 26, at 10.

assess oneself and no wrong use of the application should be done[35]

Further, the application provides for a more details on ensuring privacy as follows:

Aarogya Setu's Privacy Policy:

The Policy clarifies how some information is collected from the users to help them assess themselves and that in all aspects this shared information will be protected from any unlawful breach or theft. The privacy policy provided by the application clearly states the measures that the government will ensure are in place to protect the privacy rights and govern its people. Following the WHO Guidelines on data collection to understand how fast the virus is spreading it suggested to collect data from nation to region to understand and have it to the map. Following these guidelines which state to manage the virus encourages to have a risk-based approach, based on national risk assessments. WHO suggests that every country will have to understand their demographic growth with regard to the virus, based on certain criteria like understanding the national and regional numbers, trend and speed its growing at. While utilizing the data an outcome can be generated how fast the testing is being done, what measures are being imposed, how many people have been infected and finally whether there is widespread community transmission in another country[36]. The important pointers thus that are required not to be missed when a privacy policy is to be read have been dealt with as followed-

Information collected and manner of collection:

a) "The policy lists out the information collected at registration that includes details which is stored safely on the government's server. The data collected include (i) name; (ii) phone number; (iii) age; (iv)sex; (v) profession; and (vi) countries visited in the last 30 days. This information stored on the Server is hashed with a unique digital id (**DiD**). This identity number is utilized to identify the registered user. The geo-location is too accessed by the application".

The above clause states the first effective clause of the policy that states the information that is collected by the application. Thus, it describes how the data server of Government of India will assign a unique identity number to every user to track a person for every transaction. Thus, this clause states the method of how tracking initiates under the application.

b) "Any time two registered users come within the same range as that of the the Bluetooth device, the application is built in a way that it automatically exchanges the identity number and with it the records of information exchange time and place. This information is promised to be saved securely and not accessible by the other user. In case if any of the two persons test positive for the infection this information is uploaded on the server[37]".

Where the unique identity number has been assigned this number is then utilized for tracking further, where the Bluetooth allows sharing of this unique id, the first user's data is shared with

[35] *Id 32*, at 13.

[36] Supra Note 15, at 5.

[37] *Supra* Note 26, at 10.

the second user and the data is exchanged about their health status. Where this data is not shred with a third person, the two persons who came in contact, their devices exchange their information. Thus, where one has to mandatorily download the application, and other had volunteered, the privacy rights of the one who did not consent are infringed.

c) "Every time one completes a self-assessment test the, the Application collects location data and upload it along with the DiD to the Server[38]"

Every time a person assess himself on the application, his data is uploaded on the government server. Where the Protocol ensures about safety, is only anonymization of data sufficient enough to protect data, where other various techniques can be used to decrypt the data. Every user is again left vulnerable as he shares this data. The other important point is that the person using the application is not notified if this data has been updated or not.

d) The application continuously collects the location data and stores it securely on mobile device, a record of all the places one had visited with the time period being every 15 minute intervals. This information is uploaded to the Server along with identity number, (i) if a person tests positive for COVID-19; and/or (ii) if one self-declares his/her symptoms likely to be infected with COVID-19; and/or (iii) if the result of self-assessment test is classified as YELLOW or ORANGE. To avoid any such doubts and retain more clarity, this information is NOT uploaded to the Server. The result of self-assessment test is GREEN when someone does not show any symptom or came in direct contact with an infected person[39]".

The current clause just clarifies the earlier point and need not be discussed in more details.

Retention policy:

"All personal information collected at the time of registration is retained for as long as the account remains in existence and for such period thereafter as required under any law[40]."

The clause does not clarify as for how long the data shall be retained with the server which should ordinarily under any policy be provided to the users for their information.

"All personal information collected is 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 erased. All information collected under Clauses 1(b), 1(c) and 1(d) and uploaded to the Server will be deleted in case a person has not tested positive for COVID-19 from the Server after 45 days. All information collected under Clauses 1(b), 1(c) and 1(d) of persons who have tested positive for COVID-19 will be erased and deleted from the Server after 60 days once declared as cured."

The clause states the time for which it may be stored on the mobile device, thus can it be inferred

[38] *Supra* Note 31, at 12.

[39] *Supra* Note 26, at 10.

[40] *Id.* 37 at 15.

as the data is exchanged between the two mobile phones using Bluetooth, the exchanged information stays on the other person's phone as well.

The current clause defines the exception where the above stated clauses will not apply. Any data that is stored could be utilized for generation of datasets ensuring that the personal data is anonymized. The data generated can be used for creation of 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".

This clause need not be dealt with as it does not pose a threat to data privacy[41].

Data Security:

"The Application is equipped with in built security features to protect the confidentiality and security of every information stored on it. The Data is encrypted throughout. 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 you come in contact with is securely encrypted and are incapable of being accessed by such user"[42].

The other important pointer to be discussed under a privacy policy is the security of data. It only states that the information fed to the application will be encrypted before being uploaded on the server. Well, the Protocol too ensures that the data will be encrypted and anonymized. Thus, protecting the privacy of every user.

Disclosures and Transfer:

"Any personal information collected by the Application should not be disclosed or transferred to any third party[43]".

Finally, disclosing the data to a third party is where most often any breach occurs. Where the application states that no personal information shall be shared, the Protocol suggests the extra precautions that will be taken to protect the data like reviews, audits and using appropriate safeguards. Thus, this disclosure and transfer of data is only safe until the precautions mentioned in the policy are use.

Thus, where this application is being made popular by the government as a new technological advancement for the country, the government is required to first check the privacy loopholes because where the technology has its benefits and perks it can bring about major challenges like data theft. With no proper safeguards in any data collection application, the data is left as a prey for anyone to hack in and use it in their favor. Every day one comes across the news of data breach and data theft, thus where India has the second largest population in the world it should protect the data of its citizens from the data mines and keep the safety of its citizens at the top.

---

[41] *Supra* Note 26, at 10.

[42] *Id.* 39, at 16

[43] *Supra* Note 26, at 10.

The current application very well eases the work of the authority to go out themselves and conduct surveys. However, until the data safety is not considered a prime importance, the government should think again before putting its citizen's data out

Conclusion & scope for further research

As the pandemic continues to grow it becomes essential for a State ensure that its citizens are protected. The WHO through its guidelines on surveillance suggests that the data be collected to understand the spread, and the variation of the virus. Analyzing these guidelines and the use of contact tracing application to collect this information from every citizen can be channelized into development of the vaccination, to find out the most affected areas. The State however needs to assure time and again that at no cost is the sensitive health information collected from the people be used against them, as it's a moral duty of the State to ensure that the privacy rights are not compromised at any stage. The current widely used contact tracing application that collects data from every individual should only be used for the current purpose and not beyond it. Where the State has the authority under the Epidemic Diseases Act, and the Disaster Management Act to take strict actions to contain the virus and have everyone enjoy their right to life and health, the restrictions being imposed upon the individuals should not stand repugnant to the Constitution. Where the Constitution of India will always stand as the wall of protection of the citizen rights, the State should also act in accordance to it. Right to privacy has been read into Article 21 various times now, thus at this hour the need is to maintain a fine balance between the ensuring the privacy rights of no individual is compromised while the government continuously work towards the ensuring public health and safety. Thus, to work effectively towards this goal following suggestions can be fruitful at this hour.