CONTACT TRACING APPS *VIS-À-VIS* RIGHT TO PRIVACY IN INDIA: A CRITICAL INTROSPECTION

Payal Thaorey[*]

Anjum Ajmeri Rabbani Ansari[**]

ABSTRACT

The digitized world has made data collection and analysis crucial for understanding behavior, preferences, and offering relevant products/services. Traditional systems of data collection, processing, analysis, and protection are inadequate due to the intangible nature of data and its reusable productivity. If personal information is compromised, it violates an individual's informational privacy. Failure to address this invasion would violate their fundamental rights and expose the absence of significant Data Protection laws.

After the COVID-19 outbreak, the Indian government launched the Aarogya Setu mobile app to trace infected contacts. However, the app does not comply with the Supreme Court's anonymity condition, indicating that the compulsion to use the app might violate the privacy rights of its users. The app requires a large amount of personal information, such as name, phone number, age, sex, career, countries visited, and smoking habits, which goes against data minimization. The paper also discusses legal issues related to contact tracing apps, including the liability clause and the absence of specific laws for their usage. The government must address these issues, determine the app's legal legitimacy, and provide remedies and legal protections for individuals against data theft.

Keywords: *Aarogya setu, informational privacy, right to privacy, data protection, contact tracing*

[*] Head of Department, PostGraduate Teaching Department of Law, RTM, Nagpur University.

[**] Assistant Professor, Dr. D. Y. Patil Law College, Pune.

I. Introduction

THE FOURTH industrial revolution is transforming the intrinsic value and usefulness of data, as it is very unprecedented and unpredicted, resulting in worldwide convergence of digital, physical, and biological technology. As more and more new technologies become digital, the volume of data processed grows, with the frequency approaching that of almost like surveillance. The data collection and processing are driven by the demand for the newer technologies and for fulfilling the requirement of globalization. The increasing interaction between the communities from different parts of the world has a considerable significance in the great leap taken by technological developments.

The narrowing of distance between places and people resulted in frequent travelling of people from one part of the world to the other. Such interactions result in many good things but sometimes, these may lead to spreading of some deadly diseases too. One such example is the spreading of COVID-19 caused by severe acute respiratory syndrome coronavirus 2 (SARSCoV-2).[1] By the end of year 2019, Wuhan, a city in China recorded some cases of this disease and within one month, the disease spread to almost the whole world and thus was declared as Pandemic by the WHO.[2] This pandemic has made a devastating effect on the world and has killed more than five million among over one hundred million infected people.

[1] Chih-Cheng Lai, Tzu-Ping Shih, Wen-Chien Ko, Hung-Jen Tang, Po-Ren Hsueh, "Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and coronavirus disease-2019 (COVID-19): The epidemic and the challenges" 55 *International Journal Antimicrobial Agents* 1 (2020) *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7127800/ (last visited on Jan. 02, 2022).

[2] Anastasios Apostolos, Konstantinos Apostolos, "Tracking Applications: A Factor of Mithridatism of Personal Data and Privacy in the Post-COVID-19 Era" 1 *Disaster Medicine and Public Health Preparedness* 1 (2020).

Any such unprecedented and uncontrollable outbreak necessitates an excessively large number of measures to check the spread of the disease. In the case of COVID-19, the government and the health monitoring agencies followed the other countries and adopted measures like thermal scanning, contact tracing etc. However, probably because of the obvious priority given to the control of spread, the impact of such measures on the civil rights and liberties of the citizens could not be appropriately studied at that time.

Hence, it is very important to ensure that sensitive information like personal health data of the subjects should not reach anyone unauthorized or potential misuser. However, before the vaccine can be administered to all, the widespread use of cellphones, the Internet, and data collection are the methods adopted to improve the efficacy of a key tool viz. Digital Contact Tracing which has a potential of slowing down the spread of the disease. The data collected by this tool aids the public health authorities in drafting and implementing appropriate policies.

II. Concept of Digital Contact Tracing

Several decades of medical research tells us that when the spread of disease is bound to occur within a geographical area then a controlled measures like vaccination to pre-emptive culling helps in combating it or even helps in eradicating the infection entirely.[3] The key element which helps in controlling the spread of disease is by tracing the mobility and accessibility contact of infected persons and making others aware about it so that they can either go for early diagnosis about the infection or take safety measures. According to Eames & Keeling, contact tracing can be defined as, "an extreme form of targeted control, where the potential next-generation cases are the primary focus". Contact tracing is fundamentally linked to the individual-level spread of infection and the network of potential transmission route.[4] It allows us to keep the track of health-related information of the people with the defined networks. In the mid 1990's contact tracing methods were used to the control of sexually transmitted diseases.[5] However, the accurate modeling of contact tracing needs explicit information about the disease-transmission pathways from everyone, and hence the network of contact is required to be established.

[3] Ken T. D. Eames' and Matt J. Keeling, "Contact tracing and disease control", *The Royal Society, Proc. R. Soc. Lond. B 270, 2565-2571(2003).*
[4] *Supra* note 3
[5] Clarke, J. "Contact tracing for chlamydia: data on effectiveness", 9 *Int. J. STD AIDS* 187-191 (1998).

The concept of contact tracing is not new[6] and similar operations were carried out in the past during such pandemic situations. Plague crosses, which were placed on buildings occupied by the victims of plague, served as a rudimentary mechanism for minimizing the risk of contagion in the seventeenth and eighteenth centuries. During the AIDS crisis in the 1980s, public health officials debated the balance between contact tracing and discrimination against the LGBTQ community. The trend continues in the situation of COVID-19 as well. The significant difference between the past contact tracing and the present one may be the use of technology in the form of contact tracing applications. The idea behind having such apps were to slow down the spread of COVID-19, by providing the information related to the spread of diseases through the Internet-connected cell phones.

In March 2020, when the outbreak of COVID-19 happened the World Health Organization implemented the contact tracing with the help of software application Go. Data for providing the Global Outbreak Alert and Response Network (1),[7] to the field workers from health care system in order to assist them in monitoring the COVID-19 contact and cases. In similar lines, the Government of India too launched multiple software-based apps which can be used by the people for different services. Many of these apps eased down some of the hardships during the lockdown and helped to control the spread of SARS-CoV-2 virus.

The official Digital India account on Twitter suggests six applications, people can download and use to make their lives easier during the lockdown, namely, Safe Seniors, Quarantine watch, Bharat Interface for Money (BHIM), SMCCOVID-19 Tracker, Unified Payments Interface (UPI), Unified Mobile Application for New-age Governance (UMANG), Ayush Sanjivan, Jan Aushadhi Sugam, E-Gram Swaraj and Aarogya Setu App. BHIM[8] is the official UPI app for online payments and transfers. It's the quickest and easiest way to transfer the money online. UMANG[9] is one app where you'll find over 600 government services like Aadhaar, PAN, passport, driving license and

[6] Christopher S. Yoo and Apratim Vidyarthi, "Privacy in the Age of Contact Tracing: An Analysis of Contact Tracing Apps in Different Statutory and Disease Frameworks" 5 *University of Pennsylvania Journal of Law and Innovation* (2021).
[7] WHO, *available at*: https://iris.who.int/handle/10665/332265 (last visited on March 25, 2022).
[8] National Payment Corporation of India, Government of India, *available at:* https://www.bhimupi.org.in/ (last visited on Feb. 15, 2022).
[9] Ministry of Electronics and Information Technology (MeitY) and National e-Governance Division (NeGD), Government of India, *available at:* https://web.umang.gov.in/landing/ (last visited on Feb. 15, 2022).

more. It caters to not just central but state government services as well.[10] Ayush Sanjivani[11] App, developed by the Ministry of Ayush and MeiTY, is appropriate for studying the behavior of the population. The data obtained from this app aids in understanding the measures and steps which the public has adopted as immunity boosters.

Amid the COVID-19 outbreak, when nations all over the world proposed contact tracing applications as a way to seamlessly navigate the current issue, India too dived into it and created *Aarogya Setu 'bridge to health'*. While *Aarogya Setu* gained the highest popularity in terms of number of downloads and its usage. This is basically a digital contact tracing app. The app uses Bluetooth and GPS signals to alert users if they met a Covid-19 infected person. With the recent increase in Sexually Transmitted Diseases prevalence, the perceived risk from bioterrorism, uncontrolled virus mutation and the aim of global public-health importance the necessity and significance of contact tracing apps can never be ignored.

However, in post COVID-19 it has been seen that many private companies are now using the contact tracing method via apps to explore other than health avenues like food delivery, calling services like Zomato, true caller etc simply for the reason as they get access to the network of people. Even though privacy experts and legal professionals have voiced dissatisfaction with the above-mentioned applications of contact tracing owing to potentiality of violation of right to privacy of the users, it appears that these apps have become the most discussed topics for the season.

However, like other Internet-connected apps and gadgets, this latest generation of contact tracing Apps raises issues about data privacy. Contact tracing applications must gather some sort of location data and test result data (Sensitive personal data) and upload them to the government server to fulfil their objective of tracing the transmission of a disease. Both location data[12] means Location Data means any data processed in an electronic communications network, indicating the

[10] HT Tech, "Aarogya Setu to BHIM UPI: Govt suggests 6 apps to make life easier during lockdown" *Hindustan Times*, May 20, 2020.
[11] Ministry of Ayush, Government of India, *available at:* https://ayushnext.ayush.gov.in/detail/news/ayush-minister-launches-accr-portal-and-3rd-version-of-ayush-sanjivani-app (last visited on Feb. 15, 2022).
[12] UK Directive 2002/58/EC.

geographic position of the terminal equipment of a user of a publicly available electronic communication service and self-assessment data defines as Self-assessment data means the responses provided by that individual to the self-assessment test administered within the Aarogya Setu mobile application. are intimate and confidential, providing precise details about where data subjects travel, who they associate with, and what probable places may have caused them to test positive.[13] Many questions have arisen linked to the usage of this app and answers to them are essential for fear-free use of the App. This research will focus on addressing the research questions mentioned below:

1) Are there enough guidelines for App developers to combine the necessity of safeguarding privacy with the requirement to fulfil vital public health responsibilities through technology?
2) Do such policies or protocols released by government possess the capability of dealing with the rapidly varying requirements of specific public health crises?
3) And how do the App balance public health needs of preventing the spread of a deadly disease against individuals' privacy rights and expectations?
4) How legislation lacks mandatory imposition of the contact tracing app? And what are the issues and concerns that arise relating to lack of legislation?

Answer to these questions would be helpful to decide deficiency or efficiency of contact tracing App to combat with the Pandemic covid-19 in parallel to protect the Fundamental Right to privacy of the person because failure to address this invasion of privacy would not only stifle these technologies' transformative potential but will also exacerbate power disparities and global inequities.[14]

III. Object of the Digital Contact Tracing App

Statistics collection is regarded as an essential task for many governments and organizations throughout the world. It is indicated that to create a sound policy and have it implemented effectively, the government must have a comprehensive understanding of the situation. In India

[13] Ministry of Electronics and Information Technology, "*Notification of the Aarogya Setu data access and knowledge sharing protocol, 2020 considering the COVID-19 pandemic*, Government of India", *available at:* https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (last visited on Feb. 15, 2022).

[14] Ankit Kapoor, "Operationalizing Privacy by Design: An Indian illustration" *available at*: https://ssrn.com/abstract=3805402 (last visited on Feb. 15, 2022).

Covid Pandemic is not the first time the Government is collecting the data. After Independence legislations like Census Act, 1948[15] and Collection of Statistics Act, 2008[16] where the government has been collecting the data of persons which could fall under the category of definition of personal data under Digital Personal Data Protection Act, 2023. Census Act collects Data like Sex, Age at last birthday, Current marital status, Religion, Name of Scheduled Caste/Scheduled Tribe, Disability status, Distance and mode of travel to place of work and many more.[17] Whereas under the Collection of Statistics Act, 2008, the Central, State and Local Government has the power to collect all kinds of statistics including households and individuals.[18] The Collection of Statistics Act, 2008 enhances the scope of data collection as well as overcomes the limitations of the Collection of Statistics Act, 1953.[19]

After the technological revolution the same kind of data has been collected by Aadhar Card with legal framework, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Which collects "identity information" in respect of an individual, including his Aadhaar number, his biometric information and his demographic information.

Likewise, the Aarogya Setu App, using the cutting-edge Bluetooth technology, GPS, algorithms, and artificial intelligence, the Aarogya Setu App is next in the queue which is collecting, processing and analyzing the information of users of the App. It collects four pieces of data ("response data"): personal identifiers,[20] GPS location, Bluetooth ID,[21]and self-assessment test details. App can analyze the chances of CoronaVirus infection using an algorithm that calculates the user's contact with others. The software identifies additional devices having Aarogya Setu installed in the vicinity of a smart phone once it has been installed through an easy and user-

[15] The Census Act, 1948, as amended in 1994, (Act 37 of 1948).
[16] The Collection of Statistics Act, 2008, (Act 7 of 2009).
[17] *Data Item collected in Census*, (2011), *available at:* https://censusindia.gov.in/census_and_you/data_item_collected_in_census.aspx (last visited on Feb. 15, 2022).
[18] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act 18 of 2016).
[19] The Collection of Statistics Act, 1953 (Act 32 of 1953).
[20] Privacy Policy, Aarogya Setu Application, cl. 1(a), *available at:* https://www.aarogyasetu.gov.in/privacy-policy/ (last visited on Feb. 15, 2022).
[21] Privacy Policy, Aarogya Setu Application, cl. 1(a), 1(b) and 1(c)

friendly method. The app can accordingly calculate the risk of infection based on sophisticated parameters if any of these contacts has been tested positive.[22]

The Aarogya Setu app, developed by the Ministry of Electronics and Information Technology, Government of India, is an open-source app.[23] The Government of India launched the Aarogya Setu app claiming it as a tool to trace the movements and contacts of a COVID-19 infected person and thus combatting the COVID-19 crisis.[24] In the initial phase of its launching, Aarogya Setu was made voluntary for installation but some orders released by some state governments and the Union government seem to be intended to mandate the installation of the app at least for their employees, if not for the general public.[25] After initial mandating and passing a phase of dilemma, the Ministry of Home Affairs (MHA) released fresh guidelines on lockdown on May 17, 2020, in which the directive for downloading the app was changed from mandatory to a "best effort basis".[26]

The object behind the developing and launching the Aarogya Setu App for the people is to make them able to assess the risk of getting in contact with the people who might be affected with Covid 19. Thus, the government considered the app to be significantly useful and ensured that the App is user friendly. While on one hand these apps are made with the intention to protect the lives of people but on the other it mandates the user to surrender his sensitive personal data in this app. Thus, for achieving the purpose of Aarogya Setu App individuals' personal information is vulnerable and always at risk.

IV. Nexus Between Data Collection and Right to Privacy

In the landmark judgment of *Puttaswamy* case, the Supreme Court nine judges bench unanimously recognized that the right to privacy is a fundamental right guaranteed by the Constitution of

[22] Privacy Policy, Aarogya Setu Application, cl. 1(c) and 1(d).
[23] Andrew Clarance, "Aarogya Setu: Why India's Covid-19 contact tracing app is controversial", *BBC* (May 14, 2020), *available at:* https://www.bbc.com/news/world-asia-india-52659520 (last visited on Feb. 15, 2022).
[24] Press Information Bureau, "Aarogya Setu: A Multi-Dimensional Bridge" *Press Information Bureau* (April 02, 2020), *available at:* https://pib.gov.in/PressReleseDetailm.aspx?PRID=1610301 (last visited on Feb. 15, 2022).
[25] Ministry of Home Affairs, Order No. 40-3/2020-DM-I(A), 2020, Gen. S. R. & O.
[26] Vrinda Bhandari and Faiza Rahman, "Constitutionalism during a Crisis: The Case of Aarogya Setu" *SSRN, available at*: https://ssrn.com/abstract=3774716 or http://dx.doi.org/10.2139/ssrn.3774716 (last visited on Feb. 15, 2022).

India.[27] The report submitted by the Justice Shrikrishna committee in July 2018 on data protection clearly specifies that "processing of personal data must only be undertaken for clear, specific and lawful purposes".[28] The committee proposed that the data principal (the person whose personal data is gathered) have various rights, including the ability to revoke consent for data processing, report a breach, and have its wrongly processed data corrected by the authorities. In its decision, the Supreme Court recognized that "in the age of Big Data, the collecting and processing of personal data can disclose a lot about a person's lifestyle, choices, and preferences." [29]

Writing the plurality opinion, Chandrachud J, holds that "the right to privacy is not independent of the other freedoms guaranteed by Part III of the Constitution. It is an element of human dignity and is an inalienable natural right."[30] He focuses on the informational aspect of privacy, its connection with human dignity and autonomy. The Court noted that the deployment of such technology could be permitted in certain instances when the objective pursued by the authority is legitimate. However, despite the legitimacy in the objectives behind the deployment of such technologies, it must be ensured that the situation necessitates the deployment, and the deployment is being done in a proportionate manner. If we accumulate the test criterion given by Justice Chandrachud and Justice Kaul. J "in order to satisfy the proportionality test adopted in Puttaswamy judgment, the use of any privacy infringing technology must satisfy five criteria."

1. First, it must have a legislative basis.
2. Second, proportionality of the legitimate aims with the object sought to be achieved.
3. Third, necessity
4. Fourth, it should be a rational method to achieve the intended aim.
5. Finally, procedural safeguards against abuse of interference with rights, which echoes article 21's central requirement of having a "procedure established by law".

[27] *Justice K.S. Puttaswamy (Retd.)* v. *Union of India* (2017) 10 SCC 1.
[28] Data Protection Committee Report, "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*" (July 20, 2021).
[29] *Puttaswamy* v. *Union of India*, (2012), AIR 2017 SC 4161.
[30] Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*" SSOAR available at*: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2 (last visited on Feb. 15, 2022).

In the case of health data, the Puttaswamy (Privacy) judgment (plurality opinion authored by Justice Chandrachud) emphasized the necessity for "data protection legislation to ensure that personal data was not used to discriminate against people based on their health state." This means, when the sensitive personal data of the user is collected, it must be strictly used for the authorized and legitimate purposes without affecting the informational privacy right of an individual.

V. Contact Tracing App 'Aarogya Setu': The Assessment of Privacy Factors

To date, there are many contact tracing apps[31] and many of them hastily designed, developed, and produced. These app, were while essentially beneficial - in terms of generating a memory of proximity identifiers and urgently alerting users if they met a COVID-19 positive case.[32] However, these technologies raise ethical and privacy concerns on May 28, 2020, the World Health Organization (WHO) published an interim guideline covering the main ethical principles and requirements to achieve equitable and appropriate use of digital contact tracing technology.[33]

The privacy policy of an app is a statement, or a legal document that gives information about the ways an app provider collects, uses, discloses, and manages users' data. By law, service providers (including app providers) are required to be transparent about their data collection, sharing, and processing practices and specify how they comply with legal principles.[34] Moreover, privacy policies are the main sources that enable users to understand how their data is being handled by app developers/providers.[35]

[31] Hatamian, M., Wairimu, S., Momen, N., Fritsch L. "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps" 26 *Empir Software Eng* 36 (2021).
[32] Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C, "Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing" 368 *Science* 6491 (2020).
[33] WHO, "Ethical considerations to guide the use of digital proximity tracking technologies for covid-19 contact tracing", *available at:* https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 (last visited on Feb. 15, 2022).
[34] Hatamian M, "Engineering privacy in smartphone apps: A technical guideline catalog for app developers", 8 *IEEE Access* 35429 (2020).
[35] Reidenberg JR, Breaux T, Carnor LF, French B, "Disagreeable privacy policies: Mismatches between meaning and users' understanding", 30(1) *Berkely Technol Law J* 39 (2015).

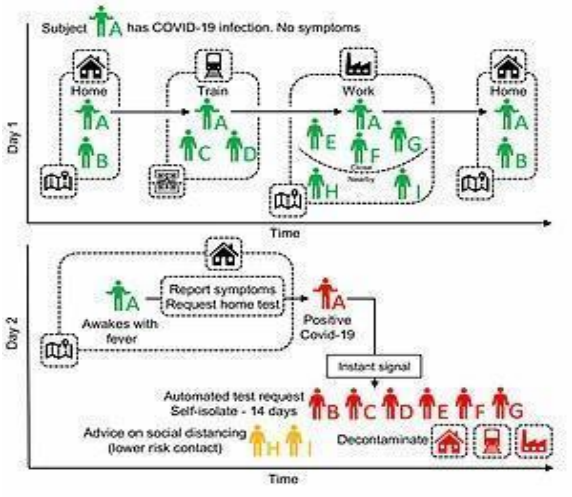
To better understand the functioning of these apps let's explore the case study of Aarogya Setu app. In this part of the paper researchers will work on the assessment of privacy factors of Aarogya Setu in line with WHO principles and its privacy policy.

To register for the Aarogya Setu app, users must create an account and provide their phone number, age, gender, profession, travel history, and whether the user is a smoker, which is saved on a government server using a unique digital identifier (DiD). The government will use this information to create anonymized, aggregated datasets for COVID-19 management, to communicate to users the probability they may have been infected with COVID-19, and to provide medical personnel information needed to carry out interventions.[36] When an individual is within range of another app user, the software uses both Bluetooth and GPS data to exchange identities and to record the time and location, which is then stored on the user's device. Every fifteen minutes, the app captures and retains users' location data locally. The app gives users the option of taking self-assessment tests that ask about symptoms, underlying conditions, recent travel, and conduct likely to have resulted in exposure, storing that information with the user's location data.[37]

The software will upload a user's location and vicinity data to the server if they test positive or have a self-assessment test that suggests possible infection. The government will use the information to pinpoint locations where outbreaks are more likely to occur, necessitating greater testing and treatment. The government will also notify other users with whom the person who has tested positive, has come into close contact.[38] Downloading the app is mandatory for citizens living in COVID-19 containment zones as well as for all working employees in both the private and public sectors.

[36] Government of India, "Aarogya Setu Privacy Policy", *available at*: https://web.swaraksha.gov.in/ncv19/privacy/ (last visited on Feb. 15, 2022).
[37] Karan Yadav, "Aarogya Setu App: Follow these simple steps to do a self-assessment test" *India Today*, May 02, 2020, *available at*: https://www.indiatoday.in/information/story/aarogya-setu-app-follow-these-simple-steps-to-do-a-self-assessment-test-1673656-2020-05-02 (last visited on Feb. 15, 2022).
[38] *Available at*: https://www.aarogyasetu.gov.in/terms-conditions/ (last visited on Feb. 15, 2022).

Fig. 1 Example proposal for a location-based COVID-19 contact tracing app[39]



Data Collection and Contact tracing app:

1) AAROGYA SETU: When a user registers with the App, the following details are collected: (i) name; (ii) phone number; (iii) age; (iv) sex; (v) profession; and (vi) countries visited in the last 30 days. This information is stored on the back-end Server, and it is hashed with a unique digital id (DiD) that is pushed to the User end App. The DiD will thereafter be used to identify the User in all subsequent App related transactions and will be associated with any data or information uploaded from the App to the Server. At registration, the User's location details are also captured and uploaded to the Server. When two registered users come within Bluetooth range of each other, their Apps will automatically exchange unique Digital IDs (DiDs) and record the time and GPS location at which the contact took place. The information that is collected from the User's App will be securely stored on the mobile device of the other registered user and will not be accessible by such other user. In the event such other registered user tests positive for COVID-19, this information will be securely uploaded from his/her mobile device and stored on the Server. Then this information is used to further carry out the contact tracing and find out all possible persons who may have come in close contact with the person who has tested positive for COVID-19. The App continuously collects your location data and

[39] *Available at*:https://en.wikipedia.org/wiki/COVID-19_apps (last visited on Feb. 16, 2022).

stores securely on your mobile device, a record of all the places you have been at 15-minute intervals. This information will only be uploaded to the server along with you DiD.

The personal information collected at the time of registration will only be used by the Government of India in anonymized, aggregated datasets for the purpose of generating reports, heat maps and other statistical visualizations for the purpose of the management of COVID-19 in the country or to provide general notifications pertaining to COVID-19 as may be required. DiD will only be correlated with personal information to communicate the probability that the person has been infected with COVID-19 and/or to provide persons carrying out medical and administrative interventions necessary in relation to COVID-19. The information collected by Aarogya Setu falls under the category of personal information. Here the question arises whether the existing technologies used in AS is parallel along with the compatibility of Aarogya Setu's privacy regulation? What kind of mechanism the authority is following to protect the data? According to SriKrishna Committee report, "The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy." Aarogya Setu was also made mandatory for the employees of private as well as public sector offices by the order passed on May 01. Hundred percent installation of this application within the containment zones was also mandated.[40] Failure to comply with the guidelines would attract penal action under sections 51 to 60 of the Disaster Management Act, 2005[41] and under section 188 of the Indian Penal Code, 1860. Under section 51(b) of the Disaster and Management Act, 2005, if a person refuses to comply with the orders given by the authorities, the person shall be imprisoned for a period that may extend to one year, or with fine, or both and under section 188 of the Indian Penal Code, 1860[42] a person shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

[40] Aryan Puri and Sanya Rawlani, "Aarogya Setu: The Right to have Rights?" 4 *International Journal of Law, Management & Humanities*, 1902 (2021).
[41] The Disaster Management Act, 2005 (Act 53 of 2005).
[42] The Indian Penal Code, 1860 (Act No. 45 of 1860)

Aarogya Setu violates the first prong of the proportionality criterion in this instance because it does not derive its legitimacy from a legislative framework to govern its operations and offer proper procedural safeguards. Due to the absence of a legislative guarantee containing a sunset clause[43] sensitive personal data about health and movement of gig workers collected by the Aarogya Setu app could potentially be misused for profiling and mass surveillance even after the COVID-19 outbreak is over. The Empowered Group shall review this Protocol after a period of 6 months from the date of this notification or may do so, at such earlier time as it deems fit. Unless specifically extended by the Empowered Group on account of the continuation of the COVID-19 pandemic in India, this Protocol shall be in force for 6 months from the date on which it is issued.

The court further went on to note that the government may collect and process the health of individuals during epidemics to design appropriate policy interventions, but such data must be anonymized. The Information Technology Act, 2000, has certain provisions that intend to protect the private information of individuals, but the said provisions are not enough to safeguard the sensitive private information, as 'Medical records' which are treated as sensitive personal information within Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Elaborately The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 issued under section 43A of the Information Technology Act, 2000 similarly classify health data as "sensitive personal data" and specify that health data can be collected and processed by body corporates only with the consent of the individual [Rule 5(1)]. The rules also impose various obligations on body corporates relating purpose limitation [Rule 5(2) and 5(5)], notice [Rule 5(3)], storage limitation [Rule 5(4)], right to access and correction [Rule 5(6)] and right to opt-out [Rule 5(7)].[44] Moreover, Information Technology rules were a novel attempt at data

[43] Ministry of Electronics and Information Technology, Government of India, "Notification of the Aarogya Setu data access and knowledge sharing protocol, 2020 in light of the COVID-19 pandemic" (May 11, 2020), *available at:* https://www.aarogyasetu.gov.in/wp-content/uploads/2020/06/mygov-1000000000981057882.pdf (last visited on Feb. 15, 2022).

[44] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

protection and the Information Technology Act, 2000, applies only to companies, not to the government. This is not the only app which is collecting the personal information of an individual but in a line, there are many more Apps launched by the State Government for their services collecting personal information which is discussed below.

2) SAFE SENIORS: RPG Life Sciences has developed an application aimed at senior adults to assist in the early detection of COVIDD-19 risk. Leading authorities in community medicine, clinical pharmacology, infectious illnesses, and Covid-19 management have all consulted on its development. In addition to helping senior adults, the application keeps the family's profile up to date.[45] Every day, the elderly or their family members must record their vital signs, past medical histories, travel and social exposure histories, and critical symptoms like fever, dry cough, etc.

3) QUARANTINE WATCH: The Karnataka revenue department created this application, which is required for those under house quarantine. This makes it easier for the Karnataka government to keep an eye on the everyday well-being of its users, including their location, health, and compliance with quarantine regulations. Users are required to update their information every day, including hourly selfies taken between 7 AM and 10 PM.[46]

4) SMC COVID-19 TRACKER: This application was developed by Surat Municipal Corporation to monitor home quarantine conditions in Surat. To share their location, users must hit an app button once every hour. This facilitates the tracking of users' movements by law enforcement agencies.[47] State agencies have developed similar software, such as COVID-19 Quarantine Monitor in Tamil Nadu, Corona Mukt Himachal in Himachal

[45] Rica Bhattacharyya, "RPG Life Sciences and Seniority launch Covid-19 risk monitoring tool for senior citizens", *Economic Times* Apr. 06, 2020, *available at*: https://m.economictimes.com/tech/software/rpg-life-sciences-and-seniority-launch- covid-19-risk-monitoring-tool-for-senior-citizens/articleshow/75013971.cms (last visited on June. 9, 2024).

[46] Samreen Ahmad, "Quarantine watch: Karnataka uses apps to keep track of people under watch" *Business Standard*, Apr 03 2020, *available at:* https://www.business-standard.com/article/technology/quarantine-watch-karnataka-uses-apps-to-keep-track-of-people-under-watch-120040201641_1.html (last visited on June.10, 2024).

[47] Ministry of Housing & Urban Affairs, Press Information Bureau "Surat Smart City takes key IT initiatives in COVID -19 management and containment" (May 29, 2020), *available at*: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1627638 (last visited on June. 9, 2024).

Pradesh, and Mahakavach in Maharashtra, to track home quarantine conditions in their respective states.

The consent of an individual for collecting and sharing of their health data, and the purposes for which health data can be used by various entities should be taken by the government. The use of digital health data for epidemic control only after it has been anonymized or de-identified.[48] As a result, even though India currently lacks a complete data privacy law, the need of safeguarding personal health data has been recognized by the judiciary and the government in many instances.

Almost all the developed democratic countries have well-framed laws for protecting their citizens from any type of personal data infringement. It is encouraging to know that many developing countries have also taken the initial steps towards the same. 137 out of 194 countries had put in place legislation to secure the protection of data and privacy. Africa and Asia show different level of adoption with 61 and 57 per cent of countries having adopted such legislations. The share in the least developed countries in only 48 per cent.[49] But unfortunately, the privacy policy and the terms of service of this contact tracing application are completely silent as to which government authority has the access to the data and till what time will the authority have access to it. Many examples are there where the government is taking care of the privacy policies of Contact Tracing Apps.

In a constitutional challenge to National Integrated Identity Management System (NIIMS)/Huduma Namba, the Kenyan national biometric identification project, the high court of Kenya held that "GPS Coordinates and DNA samples could not be collected under the cover of a general law, but in the very least would require an anchoring legislation to acquire the force of law."[50] In Israel, the Shin Bet security service's mobile phone tracking

[48] Ayushman Bharat, Health Data Management Policy Chapter, *available at:* https://abdm.gov.in:8081/uploads/health_data_management_policy_455613409c.pdf (last visited on June. 9, 2024).
[49] UN Trade and Development, "Data Protection and Privacy Legislation Worldwide by UN" *available at*: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited on June.10, 2024).
[50]Anand Venkatanarayanan, "Notes from a Foreign Field: Public Participation, Constitutional Rights, and Technological Design in the Kenyan High Court's Huduma Namba Judgment" (July 20, 2021), *available at* : https://indconlawphil.wordpress.com/2020/02/19/notes-from-a-foreign-field-public-participation-constitutional-rights-and-technological-design-in-the-kenyan-high-courts-huduma-namba-judgment/ (last visited on Feb. 15, 2022).

of confirmed carriers cannot continue, according to the High Court of Justice, unless the government legitimizes the extremely contentious practice. The tracking program "severely violates the constitutional right to privacy, and should not be taken lightly," the court added.[51]

A series of applications have been filed in the Kerala High Court contesting the validity of the MHA order demanding 100 percent coverage of the app in workplaces and confinement zones, saying that such a compulsion is unconstitutional. In the interim, it seeks "to restrain the authorities from resorting to coercive action for enforcing the mandatory use of apps". Following that, at a hearing on May 12, 2020, the court addressed the Centre orally about the feasibility of the necessary requirement, considering that the country's smartphone penetration rate does not provide fertile ground for such an imposition. The Court prima facie remarked that the petitioner has raised "valid concerns" regarding the coercive nature of the direction and asked the Centre to respond to it. The court had also asked the Centre to respond to the concerns raised regarding the privacy safeguards of the application.[52]

VI. Contact Tracing Apps: Deficient to Follow Privacy Principles

The contact tracing App, in addition to lacking a legal foundation, deviates from worldwide best practices for contact tracking applications and fails to meet data protection requirements for the following reasons:

a) Lack of Consent: Consent is a bedrock principle of privacy that informs data subjects about the kind of data the app would like to collect and asks them for consent to collect that data. Consent entails giving customers the option of agreeing to have their data used in a certain way or not using the service or application at all. However, section 6 of the Data Protect Act, 2023 requires data collection to be done in a free, specific, informed, unconditional and unambiguous manner with a clear affirmative action manner. Whereas,

[51] Stuart Winer and Times of Israel staff, "High Court: Shin Bet surveillance of virus carriers must be enshrined in law", *The Times of Israel,* Apr. 26, 2020, *available at*: https://www.timesofisrael.com/high-court-shin-bet-surveillance-of-virus-carriers-must-be-enshrined-in-law/ (last visited on Feb. 15, 2022).

[52] Livelaw News Network, "How 'Aarogya Setu' Can Be Made Mandatory When Many Workers Have No Smartphones, Kerala HC Asks Centre", *Live Law,* May 12, 2020, *available at:* https://www.livelaw.in/news-updates/kerala-hc-to-centre-how-aarogya-setu-mandatory-when-workers-have-no-smartphones-156646 (last visited on Feb. 15, 2022).

section 4 of the PDP Act, 2023 allows personal data to be processed for any lawful purpose. Interestingly, if we refer section 7 clause (f) of the same act then it allows data collection for medical emergency or threat to life or epidemics or threat to public health as a part of lawful purposes. This clearly says that any form of personal data collected through contact tracing apps is lawful and because it is for legitimate use, consent can be forceful. Further, section 17(2)(a) subsequently provides a blanket exemption from the whole law to any government agency that the government may notify, in the interests of sovereignty, security, integrity, public order, and preventing incitement. As a result, there is no way for users to deny consent or opt out.

b) Processing of Personal Data: The definition of "processing" as "a whole or partially automated operation or a series of operations conducted on digital personal data" is provided by the Digital Personal Data Protection Act, 2023, which carefully defines the term. This broad term covers a wide range of activities, such as gathering, logging, organizing, storing, modifying, retrieving, using, aligning, combining, indexing, sharing, and disclosing via transmission or another method. In addition, the notion also includes actions like limiting, deleting, or destroying data.

The DPDP Act, which does not specifically define "verifiable" permission, mandates verifiable parental approval before processing a child's personal data. If the processing is deemed safe, the Central Government may reduce the age at which parental consent is required for specific data fiduciaries, exempting them from this obligation. Furthermore, data fiduciaries have to refrain from handling personal information that could be harmful to a child's wellbeing. Section 16 (1) of Digital Personal Data Protection Act, 2023, defines personal data may also be transferred to nations outside of India, unless the Central Government specifically prohibits it. At the time of Registration for the Aarogya Setu app, it requires sharing large amounts of personal data: name, phone number, age, sex, profession, countries visited in the last 30 days and smoking habits. This is inconsistent with the principle of data minimization.

c) Lack of Transparency and Third-Party use: While it is stated that personal data gathered by Aarogya Setu is aggregated and anonymized, no publicly available information on the aggregation and anonymization procedures and methodologies is available. The Aarogya Setu protocol reads, “The anonymization standards to be used in

this process shall be developed, reviewed and updated by an expert committee appointed by the Principal Scientific Advisor to the Government of India."[53] There seems to be a failure in developing a fully formalized anonymization process. Because there is a considerable threat of re-identification unless personal data is adequately anonymized, the app must undergo extensive security testing by governmental and independent authorities.

MyGov says "the app has been built with privacy as a core principle" and the processing of contact tracing and risk assessment is done in an "anonymized manner". Mr. Singh Abhishek Singh, CEO of MyGov at India's IT ministry which built the app, says when you register, the app assigns you a unique "anonymized" device ID. All interactions with the government server from your device are done through this ID only and no personal information is exchanged after registration. Experts in the subject, however, have cast doubt on the government's assertion. India has taken decades to recognize Right to Privacy as a fundamental Right and at many instances the data of users have been compromised. But India has "a terrible history" of protecting privacy, says Mr. Pahwa, referring to Aadhaar - the world's largest and most controversial biometrics-based identity database.[54] In an interview with *The Indian Express* newspaper, former Supreme Court judge BN Srikrishna said the drive to make people use the app was "utterly illegal". "Under what law do you mandate it? So far it is not backed by any law," he told the newspaper.

d) Unauthorized Data Sharing and Risk of Function Creep: Another issue related to the App is third party sharing data where the app easily allows the authorities to upload the collected information of a person to a Indian government self-owned and self-operated "server". The government is allowed to share this personal information with "other necessary and relevant persons" for "necessary medical and administrative interventions." The Software Freedom Law Centre, a consortium of lawyers, technology experts and students, says it is problematic as it means the government can share the data with *"practically anyone it wants"*. The sharing of personal data acquired by the Aarogya Setu

[53] Government of India, "Notification of the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in light of the COVID-19 pandemic", (May 11, 2020), *available at:* https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (last visited on Feb. 15, 2022).

[54] Andrew Clarence**, "**Aarogya Setu: Why India's Covid-19 contact tracing app is controversial", *BBC News, Delhi* May 15, 2020, *available at:* https://www.bbc.com/news/world-asia-india-52659520 (last visited on Oct. 14, 2021).

app with third parties is not prohibited. The Aarogya Setu Privacy Policy does not clarify which government agencies would have access to the app's personal data. As a result, law enforcement authorities may utilize sensitive personal data acquired for contact tracing for punitive reasons. [55]

e) Cyber Security flaws (Claims of ethical hackers): It was reported that a French cybersecurity analyst had claimed that the data of positive cases could be accessed by him through the Aarogya Setu app. According to him, Aarogya Setu has many privacy and security vulnerabilities. However, the government quickly reacted to the claims, saying that hacking the Aarogya Setu app was impossible, a claim that has since been debunked.[56]

A Bengaluru-based software engineer has also managed to hack the app. The programmer who goes by the name Jay, apparently breached the app's defenses in less than four hours. This reveals gaping holes in the cyber security walls that are meant to protect personal sensitive data.[57] In line author would discuss some incidences of privacy breach in next section.

VII. Incidences of Privacy Breach

The Delhi police detained several people who are believed to be linked to the June 12 CoWIN data leak. In that incident, a Telegram bot disclosed sensitive personal information, including full name, Aadhar number, mobile number, and immunization status, of numerous citizens who had their information stored on the CoWIN platform. These advancements have taken place against the backdrop of the "Global DPI Summit" organized by the Indian Ministry of Electronics and Information Technology (MeitY) in Pune. The event, which was a component of India's agenda as the G20 president's host nation, highlighted "Digital Public Infrastructures" (DPIs) like CoWIN, UPI, and Aadhaar and highlighted how they had transformed service delivery.[58]

[55] Anmol Dhindsa and Sashwat Kaushik, "The Constitutional Case against Aarogya Setu", *SSRN* May 19, 2020, *available at*: https://ssrn.com/abstract=3610569 (last visited on Feb. 15, 2022).

[56] Tripti Dhar, "Aarogya Setu – Carrying your privacy in your hands?" *SSRN*, *available at*: https://ssrn.com/abstract=3614506 or http://dx.doi.org/10.2139/ssrn.3614506 (last visited on Feb. 15, 2022).

[57] Moneycontrol News, "Bengaluru techie hacks COVID-19 tracking app Aarogya Setu to appear 'safe' in less than 4 hours" *Money Control*, May 13, 2020, *available at:* https://www.moneycontrol.com/news/technology/bengaluru-techie-hacks-covid-19-tracking-app-aarogya-setu-to-appear-safe-in-less-than-4-hours-5262771.html (last visited on Feb. 15, 2022).

[58] Aarushi Gupta and Aman Nair," CoWIN Data Leak Is a Sign India Needs to Rethink its Digital Public Infrastructure Strategy" *The Wire*, Jun 25, 2023, *available at*: https://thewire.in/tech/cowin-data-leak-is-a-sign-india-needs-to-rethink-its-digital-public-infrastructure-strategy (last visited on June 8, 2024).

A hacking collective known as Dark Leak Market asserted in June 2021 that it has a database including the CoWIN registration details of roughly 15 crore Indians. The data can be sold again after being purchased once.[59] It's also important to note that the Aarogya Setu and Umang apps now incorporate the CoWIN portal. Even while India presents itself as a fervent supporter of DPIs internationally, incidents like this data leak serve as a sobering reminder of the discrepancy between DPI rhetoric and reality. Sadly, the very viability of these technologies has not been questioned, and DPI is being used indiscriminately for a variety of use-cases in India, from payments to immunization campaigns. There are many incidences of privacy breach its always shows the lack of concrete legislation for protection of Right to Privacy.

VIII. Lack of Legislation for Mandatory Imposition of the Aarogya Setu Application: Issues and Concerns

"Legislation is one of the most important instruments of government in organizing society and protecting citizens. It determines amongst others the rights and responsibilities of individuals and authorities to whom the legislation applies. On the other hand, a law has little or no value if there is neither discipline nor enforcement." [60]

In this part of the research paper, researchers addressed the absence of legislative underpinnings as well as certain practical governance concerns linked to the app's rollout. We begin by debating the criteria for judging presidential action in a crisis and whether unusual circumstances necessitate extraordinary actions. To answer the question whether the 'Aarogya Setu Data Access and Knowledge Sharing Protocol 2020' has any legal value? Then we explore the importance of a clear and specific law and why the Disaster Management Act or section 144 of Criminal Procedure Code fails to provide an adequate legal foundation for the app.[61]

[59] Naandika Tripathi, "How safe is your personal data? Possible data breach of CoWIN portal raises questions" *Forbes India,* June 13 2023, *available at*: https://www.forbesindia.com/article/take-one-big-story-of-the-day/how-safe-is-your-personal-data-possible-data-breach-of-cowin-portal-raises-questions/85689/1 (last visited on June 8, 2024).

[60] Office of the Auditor General Fiji "Report of The Auditor General of The Republic of Fiji" Parliamentary Paper No. 152 Of 2019.

[61] Bhandari, Vrinda and Rahman, Faiza, "Constitutionalism During a Crisis: The Case of Aarogya Setu", *SSRN available at*: https://ssrn.com/abstract=3774716 or http://dx.doi.org/10.2139/ssrn.3774716 (last visited on Feb. 15, 2022).

The government created the 'Aarogya Setu Data Access and Knowledge Sharing Protocol 2020' to ensure secure data gathering by the tracing app and restrict how such data may be shared to fulfil its goal of aiding in the battle against COVID-19. The National Disaster Management Authority's 'Empowered Group 9' is to look after the technology and data solutions in the event of a coronavirus outbreak and has written the policy. The Protocol's goal is to outline how the National Informatics Centre (NIC) would gather and exchange data generated by the Aarogya Setu app:

a) Demographic data: name, mobile number, age, profession, gender, travel history.

b) Contact Data: who the user has been nearby.

c) Self-assessment data: regarding their health and symptoms; and

d) Location data: the user's geographic position.

To answer the question whether The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 has any legal value? Raman Chima, policy director at Access Now, explained "The protocol is not a binding legal regulation; it is in effect a voluntary declaration by one group set up by the Union Government". "It does not even claim to be issued under the legal authority of the Disaster Management Act."[62]

Section 10(2)(l) of the Disaster Management Act of 2005 is being used by the government to justify the application's obligatory implementation. In response to any impending catastrophe scenario or disaster, the government can provide instructions on any topic of legislation under this provision.

It's difficult to deduce its validity from this clause since, according to entry number 97 of the list one of the Seventh Schedule of the Constitution of India, a legislation on the use and collection of data would be covered only by the Union list, thus, only the Parliament has the power to legislate on this subject matter. The National Executive Committee set up under Disaster Management Act, that issued the May 1, 2020, Guidelines directing the installation of Aarogya Setu, is not a statutory body as it is not established by an act of the parliament, and it is also pertinent to note that in the

[62] Vakasha Sachdev, "Does Govt's New Data Protocol Address Concerns Over Aarogya Setu?" *The Quint* (May 13, 2020), *available at:* https://www.thequint.com/news/india/govt-releases-new-aarogya-setu-app-data-access-protocol-experts-privacy-concerns (last visited on Feb. 15, 2022).

present case, there is no evidence of any specific parliamentary approval for directing the mandatory installation of the Aarogya Setu app.[63]

The government's directive is unclear in terms of how these recommendations will be implemented. How these guidelines will be imposed on people who do not own smartphones. Only the Ministry of the Home Affairs does not provide enough legal support. Justice BN Srikrishna, the former judge who headed the committee of experts that made the first draft of the Personal Data Protection Bill, while talking about the legality of the mandatory imposition of the application in an interview said, "Under what law do you mandate it on anyone? So far it is not backed by any law." He went to the extent of calling the mandatory use of this application "Utterly Illegal".[64] The Aarogya Setu Data Access and Knowledge Sharing protocol was issued on the of May 11, 2020, and it was issued by way of an order by the Empowered Group on Technology and Data Management.[65]

It established standards for data collecting and processing, but this is insufficient to demonstrate the legality of the application's obligatory usage. Because there is no law requiring the download of this software, it must be the primary focus of Citizens' health and their fundamental rights. Non-compliance with the mandatory installation of this application comes with penal provisions which not only hampers the liberty of the citizens but also cues coercion and compulsion, eliminating fraternity and trust.[66]

How could the administrative authorities keep these penal provisions when the App has no Legal validity? Again, this would be a violation of your fundamental Rights and showing the excessive use of arbitrary powers which violates the Natural rule of justice. The very recent example in Uttar Pradesh where the UP police issued new guidelines, action will be taken against people going

[63] *Supra* note 42.
[64] Apurva Vishwanath," Mandating use of Aarogya Setu app illegal, says Justice B N Srikrishna" The Indian Express, May 13, 2020, *available at:* https://indianexpress.com/article/india/aarogya-setu-app-mandate-illegal-justice-b-n-srikrishna-6405535/ (last visited on Feb. 15, 2022).
[65] *Supra* note 56.
[66] *Supra* note 66.

outdoors without installing the Aarogya Setu app in Gautam Buddh Nagar in western Uttar Pradesh.[67]

"If smartphone users do not have the 'Aarogya Setu' app installed on their mobile phones, then that will be punishable and considered a violation of the lockdown directions," Additional Deputy Commissioner of Police, Law and Order, Ashutosh Dwivedi said. What could be the protective measures the machinery has, to prevent the abuse of such data and alleviate worries about surveillance?[68] This kind of statement in the media is a clear violation of fundamental Rights.
The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020[69] lays down certain principles regarding the collection, processing, and sharing of personal data.[70] However, the Protocol does not have the status of law, nor can it receive any formal basis from the Disaster Management Act, 2005. More significantly, it does not aim to bestow any legal standing to the app itself. As a result, the Protocol cannot be construed as establishing legal grounds for the use of the Aarogya Setu app.

If the Protocol is violated and the information is abused, there are no enforcement measures in place. To understand the policy of protocol, for an example, If a government department shares your information with a private company without your permission, or shares information with a research organization that hasn't been properly anonymized, or if a private company that received the information correctly forwards it on to others, like giving your health and contact data to an insurance company or advertiser if your privacy violates due to sharing of your health data which falls under the category of Sensitive Personal Data the difficulties are in filing a complaint in this case would arise from:
(a) The Liability clause (the government has effectively absolved itself from any legal liability in case of a breach).

---

[67] ET Government, "COVID-19 Crisis: Not installing 'Aarogya Setu' app becomes a criminal offence in UP", *Economic Times*, May 06, 2020, *available at:* https://government.economictimes.indiatimes.com/news/digital-india/covid-19-crisis-not-installing-aarogya-setu-app-becomes-criminal-offence-in-up/75566422 (last visited on Feb. 15, 2022).
[68] Ankit Kapoor, "Operationalizing Privacy by Design: An Indian illustration" *SSRN, available at*: https://ssrn.com/abstract=3805402 (last visited on Feb. 15, 2022).
[69] *Supra* note 68.
[70] Aditi Agrawal, "All You Need to Know About MEITY's Data Access and Sharing Protocol For Aarogya Setu", May, 11, 2020, *Medianama available at:* https://www.medianama.com/2020/05/223-meity-aarogya-setu-data-access-sharing-protocol/ (last visited on Feb. 15, 2022).

(b) Absence of a data protection law or any specific law for the usage of Aarogya Setu.

Another aspect of the Protocol, which has been subject to strong criticism is the fact that it includes a 'sunset clause' for the protocol itself in Para 10. Under this, the Empowered Group will review the Protocol after six months and decide whether it needs to be extended otherwise it will cease to operate. However as pointed out by Nikhil Pahwa, founder of Media Nama, "there is no sunset clause for the use of the app itself. There is a sunset date for the protocol, not the app. This creates further distrust as for any data collected after the protocol ends, the protocol itself will not apply."

IX. Conclusion

The government's poor track record on privacy, lack of transparency, and lack of data protection laws have raised serious concerns. The government must address the following primary issues: (a) where does the app get its legal legitimacy from, given that there are obvious reasons for the invasion of privacy? (b) Legal protections against data theft. The government must address this issue.

These concerns must be addressed openly by the government. Transparency, accountability, protecting individual rights, identifying organizational measures and compliances to be done, to mention a few guiding elements. It is all more vital to establish a data protection legislative framework in the current environment of contact tracing applications. At the end of the day, no amount of sophisticated technology will be able to save us from this unprecedented threat to our health and economic stability. At most, the most apparent technological solutions will be of little assistance. At the very least, it is the responsibility of their creators to guarantee that they cause no harm. However, under the App's privacy policy, registered users' access, correction, and erasure rights are limited to only the personal information that they have provided. As a result, in the absence of regulation, adherence to the privacy principles is insufficient.

Finally, the use of contact tracking applications will put the balance between government monitoring and consumer privacy to the test. The necessity for data protection laws is clear in India for protection of the fundamental right that is “Right to Privacy”.