IN THE HIGH COURT OF KARNATAKA AT BENGALURU

DATED THIS THE 25TH DAY OF JANUARY, 2021

PRESENT

THE HON'BLE SHRI ABHAY S. OKA, CHIEF JUSTICE

AND

THE HON'BLE SHRI JUSTICE S. VISHWAJITH SHETTY

WRIT PETITION NO.7483 OF 2020 (GM-RES-PIL)

Between:

Anivar A Aravind
S/o Aravindakshan A.K.
Aged about 36 years
F1, Sai Ram, 10
Sundara Murthy Road
Cox Town, Bangalore – 560 005

...Petitioner

(By Shri Colin Gonsalves, Senior Advocate
for Shri Clifton D'Rozario, Advocate)

And:

1 . Ministry of Home Affairs
Jai Singh Marg
Hanuman Road Area
Connaught Place
New Delhi – 110 001

2. The Ministry of Railways
Through the Secretary
Rail Bhawan, Rafi Marg
New Delhi – 110 001

3. Ministry of Civil Aviation
Through the Secretary

Rajiv Gandhi Bhawan
Block-B, Safdarjung Airport Area
New Delhi – 110 003.

4. Airports Authority of India
Through the Secretary
Rajiv Gandhi Bhawan, Block-B
Safdarjung Airport Area
New Delhi – 110 003

5. State of Karnataka
Represented by The Secretary
Home Department
II Floor, Vidhana Soudha
Bangalore – 560 001

6. Ministry of Electronics and Technology
Represented by the Secretary
Electronics Niketan,
6, CGO Complex, Lodhi Road
New Delhi – 110 003

7. National Informatics Centre
Through its Director General
A-Block, CGO Complex
Lodhi Road, New Delhi – 110 003

8. Union of India
Through Secretary
Ministry of Health and Family Welfare
Nirman Bhawan, Delhi – 110 001

9. Bangalore Metro Rail Corporation Ltd (BMRCL)
Through Managing Director
Third Floor, BMTC Complex,
KH Road, Shanthi Nagar
Bangalore – 560 027

Respondents

(By Shri M.B. Nargund, Additional Solicitor General of India
along with M.N. Kumar, Central Government Counsel

for Respondents No.1, 3, 6 to 8,
Shri V.K. Narayanaswamy – Advocate for R2,
Shri M.B. Anirudh – Advocate for R4,
Shri Vijay Kumar A Patil, Additional Government
Advocate for R5,
Shri Basavaraj V. Sabarad for R9)

This Writ Petition is filed under Article 226 of the Constitution of India praying to direct the respondent Authorities to make the use of Aarogya Setu application by citizens voluntary and etc.

This Writ Petition having being heard and reserved for passing order on prayer for interim relief, coming on for pronouncement of order, this day, **the Chief Justice** made the following:

O R D E R

OVERVIEW:

On 19th August, 2020 rule *nisi* has been issued in this petition. Thereafter, submissions were heard from time to time on the prayer for interim relief. The submissions were lastly heard on 17th December, 2020 and order was reserved.

2. The issue in this writ petition concerns *Aarogya Setu app*lication (for short, 'the *Aarogya Setu app')* introduced by the Government of India after the nationwide lockdown was announced by the Hon'ble Prime Minister on 24th March, 2020. The National Informatics Centre ('NIC' for short)-seventh respondent launched the *Aarogya Setu app* on 2nd April, 2020

which is stated to have been downloaded by more than one hundred million users. One of the issues involved is whether the Government of India has a right to use the personal data of *Aarogya Setu app* users on the app and whether it can transfer/ share the data without obtaining the informed consent of the users. On 1st May, 2020, an order was made by the Union Home Secretary, the Ministry of Home Affairs, in his capacity as the Chairperson of the National Executive Committee of the National Disaster Management Authority (for short, 'the NDMA') under the Disaster Management Act, 2005 (for short, 'the said Act of 2005'). The said order was passed in exercise of powers under Section 10 (2) (l) of the said Act, 2005, by which, new guidelines were issued on lockdown which were annexed to the said order. The guidelines appended to the said order provided for ensuring 100% coverage of the *Aarogya Setu app* amongst the residents of Containment Zones. On 11th May, 2020, an order was issued by the Chairperson, Empowered Group on Technology and Data Management which was constituted by the National Executive Committee of the NDMA. By the said order of 11th May, 2020, directions were issued in the name

and style of "the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020" (for short, 'the said protocol').

3. Before adverting to the submissions made across the Bar, it is necessary to quote the prayers made in this writ petition both for final relief and interim relief which read thus:

"PRAYER

Wherefore, the petitioner in the above case most respectfully pray this Hon'ble Court be pleased to issue:

I. A writ of mandamus or any other appropriate writ or order directing the respondent authorities to make the use of Aarogya Setu application by citizens voluntary;

II. A declaration to the effect that the Aarogya Setu app cannot be mandated for accessing any Government service or facility;

III. A writ of mandamus or any other appropriate writ or order directing respondents 6 and 7 to release the complete and corresponding source code of the current and future versions of the mobile application Aarogya Setu as well as the corresponding application on its server;

III-A. Direction to the respondents to delete and destroy the already collected data including the data collected at the time of registration once the pandemic phase is declared as over by the World Health Organisation or the Ministry of Health and Family Welfare.

III-B. Direct the respondents not to transfer or share personal data and sensitive personal data of citizens collected through the Aarogya Setu application to third parties except when it is necessary for the treatment purpose of a patient, and even such shared data should be deleted once the pandemic phase is over.

III-C. To set aside Clause 3(vii) of Annexure N issued by the 8th respondent.

III-D. To direct the respondent No.9 not to make it mandatory for commuters to use Aarogya Setu to travel in Bangalore Metro.

IV. Grant any other relief that this Hon'ble Court deems fit in facts and circumstances of the case, in the interest of justice.

V. For an order permanently injuncting the respondents from proceeding with the Aarogya Setu app and with the data collected, in any manner,

whether the collection of data from members of the public is stated to be voluntary or involuntary.

VI. For an order directing the respondents to permanently delete all the data collected through the Aarogya Setu app, including the data transferred to third parties.

INTERIM PRAYER

The petitioner prays that this Hon'ble Court be pleased to grant an interim order:

1. Staying Clause 15 of National Directives for COVID-19 Management included as Annexure 1 in Annexure-E order; and
2. Directing the respondents not to deny any service to a citizen for not installing the Aarogya Setu application, pending disposal of this Writ Petition.
3. For an order restraining the respondents during the pendency of this petition from proceeding with the Aarogya Setu app and with the data collected, in any manner, whether the collection of data from members of the public is stated to be voluntary or involuntary".

4. Prayer III-C refers to clause 3 (vii) of Annexure-N which is a Standard Operating Procedure (for short, 'SOP') issued by the Government of India, Ministry of Health and Family Welfare on 4th June, 2020 relating to the preventive measures to contain

spread of COVID-19 in the offices. Clause 3 (vii) of the said SOP seeks to make the installation and use of the *Aarogya Setu app* by the employees mandatory.

5. We must note here that by the Order dated 19th October, 2020, this Court directed that till the petition is heard on the prayer for interim relief and in the absence of any legislation, neither the State Government nor the Central Government, its agencies or instrumentalities can deny any benefit of any services to a citizen only on the ground that he has not installed the *Aarogya Setu app* on his cell phone. As far as the prayer made in clause (2) for interim relief is concerned, we must note here that the Government of India (8th respondent), Airports Authority of India (4th respondent) and Bengaluru Metro Rail Corporation Limited (9th respondent) have taken a clear stand that installation and use of the *Aarogya Setu app* is not mandatory for those who want to avail facilities provided by them. The order dated 12th June, 2020 clearly records that the passengers who wish to travel by Air or Railway are not mandatorily required to download and install the *Aarogya Setu app* as a condition precedent for travelling. The Order dated 3rd August, 2020 records the statement made by the Government of

India in the memo dated 2nd August, 2020 wherein it is stated that installation of the *Aarogya Setu app* is voluntary in nature which is intended to help the users to have reduced risk of infection of COVID-19. The Order dated 19th August, 2020 records the submission made by the learned counsel appearing for the Airports Authority of India to the effect that downloading and installation of the *Aarogya Setu app* for Air travelers is not mandatory and it is optional. Thus, the second prayer for interim relief is virtually worked out. The same is the case as regards the first prayer for interim relief. Thus, what remains for consideration is the third prayer for interim relief.

6. Detailed submissions have been made by Shri. Colin Gonsalves, the learned senior counsel representing the petitioner and Shri. M.B. Nargund, Additional Solicitor General of India, representing the first, third, sixth to eighth respondents. It is necessary to briefly refer to the said submissions.

SUBMISSIONS OF THE PETITIONER:

7. The learned Senior Counsel appearing for the petitioner heavily relied on what is held by the Apex Court in the case of

Justice K.S. Puttaswamy (retired) –vs Union of India[1]. He submitted that a data controller is not entitled to disclose the data concerning personal information of an individual to third parties without seeking informed consent from the individual for such a disclosure. He relied upon the provisions of the Personal Data Protection Bill, 2019 (for short "the said Bill").

8. He submitted that the claim of the Government of India that anonymisation has been made is not substantiated, as it is not verified or checked by any Authority. He submitted that the Source Code both on the server side and the device side has not been disclosed. He pointed out the scheme of the said Bill. He relied upon various articles and contends that *Aarogya Setu app* is the least secured app and submitted that the statements made in the affidavits filed by the Government of India are not true. He pointed out the entire procedure right from the stage of registration of an individual on the *Aarogya Setu app* and submitted that as can be seen from the *Aarogya Setu app* itself, it is evident that the personal data such as location details, name, phone number, age, sex, occupation/profession, countries recently visited by a person who downloads *Aarogya*

[1] (2017) 10 SCC 1

Setu app and who registers himself is uploaded on the Government of India server. He submitted that at the stage of registration itself, the location details are captured and uploaded on the server. He pointed out that when two registered users come within the Bluetooth range of each other, their apps will automatically exchange DiDs and record the time and GPS location at which the contact took place. He submitted that the stand taken by the Government of India that the data so collected from the registered user would remain on his cell phone and such data collected from the registered user will not be uploaded on the Government of India server, unless the registered user is tested positive for COVID-19 is not correct. He also invited our attention to the retention clause in the said protocol. He also pointed out the provision regarding sharing of response data containing personal data by NIC with various Government departments and Public Health Institutions of the Government. He submitted that there is no sunset clause for the data collected. The sunset clause provides that unless specifically extended by the Empowered Group on account of the continuation of COVID-19 pandemic in India, the said

protocol will be in force for six months from the date on which it was issued.

9. He submitted that merely by clicking the buttons and icons forming a part of *Aarogya Setu app,* the user does not give informed consent for transferring and sharing of his personal data. The learned counsel, therefore, prayed for interim relief in terms of prayer 3 of the interim prayers.

SUBMISSIONS OF THE CONTESTING RESPONDENTS:

10. The learned Additional Solicitor General of India has taken us through the stand taken in the statement of objections of the Government of India in which it is stated that it is not at all mandatory to download *Aarogya Setu app*, as clearly provided in various Orders of National Executive Committee appointed under the said Act of 2005. He pointed out that there is a categorical statement made to the effect that no services are denied to the citizen merely on the ground of non-installation of *Aarogya Setu app.* He submitted that *Aarogya Setu app* is only one of the measures for preventing spread of pandemic COVID-19. He invited our attention to the Order dated 11th May, 2020 issued by the Chairperson, Empowered Group on

Technology and Data Management which was constituted by the NDMA and submitted that all the personal information is securely encrypted and stored on the server. He also submitted that test of proportionality will have to be applied. He submitted that the said protocol has been issued by the Chairperson, Empowered Group on Technology and Data Management which clearly clarifies the position. He submitted that the claim of the petitioner that all personal data of the users of *Aarogya Setu app* is shared has no foundation at all, inasmuch as, all the safeguards have been provided. He submitted that *Aarogya Setu app* is one of the important tools for locating those who are infected with COVID-19. It is a tool for contact tracing. He reiterated that as the downloading and use of *Aarogya Setu app* is not mandatory for enabling the citizen to avail the benefits and services, there is no ground to grant any interim relief sought by the petitioner. He has also pointed out certain paragraphs of the decision of the Apex Court in the case of ***Justice K.S. Puttaswamy*** (supra) and subsequent decisions.

CONSIDERATION OF SECOND PRAYER FOR INTERIM RELIEF:

11. In this case, we are dealing with a mobile application designed and launched by NIC which is a wing of the

Government of India. The Aarogya Setu app is not like any other ordinary private mobile application available, which can be downloaded by the citizens. The reason is that in the Standard Operating Procedures published by the National Executive Committee of the National Disaster Management Authority contain a reference to requirement of downloading of Aarogya Setu app. Even in the Standard Operating Procedures/ instructions issued by many agencies and instrumentalities of the State, requirement of downloading of Aarogya Setu app is suggested. The requirement may not be mandatory. But the citizens are being suggested or advised to download and install Aarogya Setu app as a measure for preventing spread of COVID-19. Moreover, in view of the frequent appeal made by the Government, large number of citizens have installed the app on their mobile phones. Therefore, it is very necessary for this Court to examine the question whether, *prima facie*, the right of privacy guaranteed by Article 21 of the Constitution of an individual citizen who installs Aarogya Setu app is violated by the Government of India and agencies or instrumentalities of the State. As the said Aarogya Setu app is creation of Government of India, the question which we have to answer is whether, *prima*

facie, the data of an individual available on the Aarogya Setu app is being used or shared without informed consent of the user. If the data of an individual which is available on the Aarogya Setu app is shared with third parties without the informed consent of the user to third parties or used without obtaining informed consent of such an individual, it will be a violation of his right of privacy conferred upon him by Article 21 of the Constitution.

12. We have considered the submissions made across the Bar. At this stage, we are not finally deciding the main issues raised in the petition. Therefore, we are recording only *prima facie* and tentative findings for the purposes of considering the prayer for interim relief. Firstly, we deal with the 2nd prayer for interim relief in the amended writ petition which reads thus:

> "2. Directing the respondents not to deny any service to a citizen for not installing the Aarogya Setu application, pending disposal of this Writ Petition."

13. On 19th October, 2020, this Court directed by an interim order that till the petition is heard for consideration of the prayer for interim relief and in the absence of any legislation, neither the

State Government nor the Central Government or its agencies or instrumentalities can deny any benefits to a citizen only on the ground that he has not installed the *Aarogya Setu app* on his cell phone.

14. The Government of India has filed statement of objections which is supported by verifying affidavit. Clause (iv) and (v) of paragraph-6 of the statement of objections are relevant which read thus:

> "iv. As per the said order, it is not at all mandatory to download Aarogya Setu application and various phases of Unlock Orders issued by the National Executive Committee, under the Disaster Management Act, 2005. As per the said orders, no services are denied to the citizens merely on the grounds of not installing the *Aarogya Setu app*. Therefore, the statements made by petitioner in this regard are misconceived. The *Aarogya Setu application* is one of the preventive measures for containing spread of COVID-19. The State and/or its instrumentalities will follow the orders of the National Executive Committee. The apprehension of the petitioner that the State and its instrumentalities would deny services if, the *Aarogya Setu application* is not installed, is misplaced and misconceived without any basis.

v. The SOP dated 04/06/2020, on preventive measures in Shopping Malls to contain spread of COVID-19, issued by the Ministry of Health and Family Welfare, in which clause 3 (vii) forms part of Generic preventive measures which states that "installation and use of *Aarogya Setu app* shall be advised to all". It is very clear that it is only advisory in nature. The said SOP dated 04/06/2020 is annexed hereto as **Annexure-R12** and hence, the prayer No.1 does not survive for consideration."

(underlines supplied)

Again, in paragraph 19 of the statement of objections, it is stated thus:

"19. Averments in paragraph Nos 6 and 7 of the memorandum of Writ Petition are misconceived. At the cost of repetition, it is reiterated that the National Executive Committee has not passed any order, mandating the use of *Aarogya Setu application* for availing any Government services. Further, the Governments and Authorities would follow the orders passed by the National Executive Committee, in relation to measures to be taken for containing spread of COVID-19. Respondent Nos. 2, 3 and 4 also have not mandated the use of *Aarogya Setu application*, for availing travel services. The App does not violate the privacy of any individual. The right to

> privacy has not been compromised as adequate privacy protections have been built in the App. The App has built in privacy principles of right to access and correct personally identifiable information for registered users, use limitation, purpose limitation, data minimization, data retentions and data security."
>
> (underlines supplied)

15. Thus, the second prayer for interim relief stands answered. We, therefore, make it clear that no citizen can be denied the benefits of any Government services or the services rendered by any of the agencies or instrumentalities of the State solely on the ground that he has not downloaded and installed *Aarogya Setu app.* We must also note here that the Airport Authority of India and the BMRCL have also clarified the position in categorical terms that travel services will not be denied by them on the ground that the persons who seeks to avail of such services have not downloaded and installed the *Aarogya Setu app.*

CONSIDERATION OF THIRD PRAYER FOR INTERIM RELIEF:

16. Now, we come to the third prayer for grant of interim relief which reads thus:

> "3. For an order restraining the respondents during the pendency of this petition from proceeding with the Aarogya Setu app and with the data collected, in any manner, whether the collection of data from members of the public is stated to be voluntary or involuntary."

17. We may note here that reliance placed by the petitioner on the said Bill introduced in the Parliament will not help the petitioner, as it is not yet converted into a legislation.

18. Basically, third prayer is founded on the contentions that the data uploaded by an individual who downloads and installs *Aarogya Setu app* on his mobile phone is being illegally stored and/or transferred by the Government of India without obtaining his informed consent and, therefore, such illegal transfer of the personal data of an individual is violative of the right to privacy guaranteed by Article 21 of the Constitution of India. In support of this contention, reliance is placed on what is held by the Apex Court in the case of ***Justice K.S. Puttaswamy*** (supra). The conclusions drawn by the Apex Court in the case of ***K.S. Puttaswamy*** (supra) have been summarized in paragraph 316 onwards of the said decision. The observations made by the

Apex Court in paragraphs 320 to 328 are relevant for this petition which read thus:

> **"T. *Our conclusions***
>
> **320.** Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III.
>
> **321.** Judicial recognition of the existence of a constitutional right to privacy is not an exercise in the nature of amending the Constitution nor is the Court embarking on a constitutional function of that nature which is entrusted to Parliament.
>
> **322.** Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level privacy subserves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty.
>
> **323.** Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left

alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being.

324. This Court has not embarked upon an exhaustive enumeration or a catalogue of entitlements or interests comprised in the right to privacy. The Constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the Rule of Law. The meaning of the Constitution cannot be frozen on the perspectives present when it was adopted. Technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present. Hence the interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its

content bearing in mind its basic or essential features.

325. Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the threefold requirement of (*i*) legality, which postulates the existence of law; (*ii*) need, defined in terms of a legitimate State aim; and (*iii*) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

326. Privacy has both positive and negative content. The negative content restrains the State from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the State to take all necessary measures to protect the privacy of the individual.

327. Decisions rendered by this Court subsequent to *Kharak Singh*, upholding the right to privacy would be read subject to the above principles.

328. Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the State but from non-State actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union Government while designing a carefully structured regime for the protection of the data. Since the Union Government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union Government having due regard to what has been set out in this judgment."

(underlines supplied)

While discussing in detail various facets of privacy, in paragraph 300 onwards, the Apex Court has discussed the issue of informational privacy. The finding recorded by the Apex Court in paragraph 300 is relevant which reads thus:

S. Informational Privacy

> **"300.** Ours is an age of information. Information is knowledge. The old adage that "knowledge is power" has stark implications for the position of the individual where data is ubiquitous, an all-encompassing presence. Technology has made life fundamentally interconnected. The internet has become all-pervasive as individuals spend more and more time online each day of their lives. Individuals connect with others and use the internet as a means of communication. The internet is used to carry on business and to buy goods and services. Individuals browse the web in search of information, to send e-mails, use instant messaging services and to download movies. Online purchases have become an efficient substitute for the daily visit to the neighboring store. Online banking has redefined relationships between bankers and customers. Online trading has created a new platform for the market in securities. Online music has refashioned the radio. Online books have opened up a new universe for the bibliophile. The old-fashioned travel

> agent has been rendered redundant by web portals which provide everything from restaurants to rest houses, airline tickets to art galleries, museum tickets to music shows. These are but a few of the reasons people access the internet each day of their lives. Yet every transaction of an individual user and every site that she visits, leaves electronic tracks generally without her knowledge. These electronic tracks contain powerful means of information which provide knowledge of the sort of person that the user is and her interests. Individually, these information silos may seem inconsequential. In aggregation, they disclose the nature of the personality: food habits, language, health, hobbies, sexual preferences, friendships, ways of dress and political affiliation. In aggregation, information provides a picture of the being: of things which matter and those that do not, of things to be disclosed and those best hidden.

Paragraphs 303 and 304 are also relevant which read thus:

> **303.** The age of information has resulted in complex issues for informational privacy. These issues arise from the nature of information itself. Information has three facets: it is non-rivalrous, invisible and recombinant. Information is non-rivalrous in the sense that there can be simultaneous users of the good — use of a piece of information by one person does not make it less available to

another. Secondly, invasions of data privacy are difficult to detect because they can be invisible. Information can be accessed, stored and disseminated without notice. Its ability to travel at the speed of light enhances the invisibility of access to data, "information collection can be the swiftest theft of all". Thirdly, information is recombinant in the sense that data output can be used as an input to generate more data output.

304. Data mining processes together with knowledge discovery can be combined to create facts about individuals. Metadata and the internet of things have the ability to redefine human existence in ways which are yet fully to be perceived. This, as *Christina Moniodis* states in her illuminating article, results in the creation of new knowledge about individuals; something which even she or he did not possess. This poses serious issues for the Court. In an age of rapidly evolving technology it is impossible for a Judge to conceive of all the possible uses of information or its consequences:

"… The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our State becomes an "information State" through increasing reliance on information—such that information is described as the "lifeblood that sustains political,

social, and business decisions. It becomes impossible to conceptualize all of the possible uses of information and resulting harms. Such a situation poses a challenge for courts who are effectively asked to anticipate and remedy invisible, evolving harms."

The contemporary age has been aptly regarded as "an era of ubiquitous dataveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology". It is also an age of "big data" or the collection of data sets. These data sets are capable of being searched; they have linkages with other data sets; and are marked by their exhaustive scope and the permanency of collection. The challenges which big data poses to privacy interests emanate from State and non-State entities. Users of wearable devices and social media networks may not conceive of themselves as having volunteered data but their activities of use and engagement result in the generation of vast amounts of data about individual lifestyles, choices and preferences. Yvonne McDermott speaks about the quantified self in eloquent terms:

"… The rise in the so-called 'quantified self', or the self-tracking of biological, environmental, physical, or behavioural information through tracking devices, Internet-of-things devices, social network

> data and other means (?Swan.2013) may result in information being gathered not just about the individual user, but about people around them as well. Thus, a solely consent-based model does not entirely ensure the protection of one's data, especially when data collected for one purpose can be repurposed for another."

Paragraph 306 of the decision considers the balance between data regulation and individual privacy wherein it has been observed by the Apex Court that the issues requiring delicate balances to be drawn between the legitimate concerns of the State on one hand and individual interest in the protection of privacy on the other. Paragraph 307 of the said decision is also relevant which reads thus:

> **"307.** The sphere of privacy stretches at one end to those intimate matters to which a reasonable expectation of privacy may attach. It expresses a right to be left alone. A broader connotation which has emerged in academic literature of a comparatively recent origin is related to the protection of one's identity. Data protection relates closely with the latter sphere. Data such as medical information would be a category to which a reasonable expectation of privacy attaches. There may be other data which falls outside the reasonable

> expectation paradigm. Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual. This is evident from the emphasis in the European data protection regime on the centrality of consent. Related to the issue of consent is the requirement of transparency which requires a disclosure by the data recipient of information pertaining to data transfer and use."
>
> (underlines supplied)

19. Paragraph 309 of the said decision deals with a complex exercise of formulation of a regime for data protection which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data subserves together with the legitimate concerns of the State. In paragraph 311, the Apex Court has taken a note of the fact that apart from national security, the State may have justifiable reasons for collection and storage of data. In paragraph 314, the Apex Court has quoted nine privacy principles in a framework for protection of privacy concerns which are proposed by a group of experts under the auspices of erstwhile Planning Commission. Out of the nine principles, two are relevant which are at paragraphs 314.1 and 314.2. Paragraphs 314.1 and 314.2 read thus:

> "314.1. **Notice:** A data controller shall give simple-to-understand notice of its information practices to all individuals in clear and concise language, before personal information is collected.
>
> 314.2. **Choice and consent:** A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices."

20. Two important privacy principles are quoted above. The first one is that a data controller is required to give simple-to-understand notice of its information practices to all individuals in clear and concise language, before personal information is collected. The second principle is of taking individual consent only after providing notice of its information practices and to give an individual, choices of 'opt-in/opt-out' regarding providing personal information. In view of the right of privacy guaranteed by the Constitution of India, unless there is an informed consent of the users, the data of individual users cannot be used or shared, especially, because the data concerned involves health condition of the user.

21. We have carefully perused the annexure R1 to additional counter reply dated 10th December, 2020 filed by the Government of India. Annexures thereto are the printouts of contents of Aarogya Setu app. The *Aarogya Setu app* itself contains information regarding the practices in the form of "Aarogya Setu terms and conditions" and "Privacy Policy". These are the two material documents. A copy of "Aarogya Setu terms and conditions" is produced as Annexure-R5 along with the statement of objections filed on 7th November, 2020. The said document can be accessed on the *Aarogya Setu app*. Clause-4 of the said document refers to 'privacy'. By clicking on the said word, the privacy policy can be read. There are two more material clauses apart from clause-4 in the terms and conditions. The said clauses are clauses-1 and 2 regarding 'service overview' and 'requirements for use'. A copy of 'Privacy Policy' available on the Aarogya Setu app has been produced as Annexure-R4. For ready reference and for the purpose of convenience, the same is extracted here below:

"PRIVACY POLICY

When you use Aarogya Setu (**App),** some personal information is collected from and about you. We are committed to protecting the security of this

information and safeguarding your privacy. This privacy policy sets out the details of the personal information collected, the manner in which it is collected, by whom as well as the purposes for which it is used. At registration you accepted the terms of this Privacy Policy and your use of the App signifies your continued acceptance thereof. This Privacy Policy may be revised from time to time and you will be notified of all such changes. In order to use the App, you will be required to consent to the terms of the Privacy Policy as revised from time to time.

1. **INFORMATION COLLECTED AND MANNER OF COLLECTION.**

a. When you register on the App, the following information is collected from you and stored securely on a server operated and managed by the Government of India (**Server) –** (i) name; (ii) phone number; (iii) age; (iv) sex; (v) profession; and (vi) countries visited in the last 30 days. This information will be stored on the Server and a unique digital id (DID) will be pushed to your App. The DiD will thereafter be used to identify you in all subsequent App related transactions and will be associated with any data or information uploaded from the App to the Server. At registration, your location details are also captured and uploaded to the Server.

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

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

d. The App continuously collects your location data and 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 your DiD, (i) if you test positive for COVID-19; and/or (ii) if your self-declared symptoms indicate that you are likely to be infected with COVID-19; and/or (iii) if the result of your self-assessment test is either YELLOW or ORANGE. For the avoidance of doubt, this information will NOT be uploaded to the Server if you are not unwell of if it the result of your self-assessment test is GREEN.

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

2. USE OF INFORMATION

a. The personal information collected from you at the time of registration under Clause 1 (a) above, will be stored on the Server and only be used by the Government of India in anonymized, aggregated datasets for the purpose of generating reports, heat maps and other statistical visualizations for the purpose of the management of COVID-19 in the country or to provide you general notifications pertaining to COVID-19 as may be required. Your DiD will only be co-related with your personal information in order to communicate to you the probability that you have been infected with COVID-19 and/or to provide persons carrying out medical and administrative interventions necessary in relation to COVID-19, the information they might need about you in order to carry out such interventions.

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

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

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

e. The information securely uploaded and stored on the Server under Clause 1(e) will be used to calculate the probability of those who have come in contact with you being infected with COVID-19.

f. The information collected under Clause 1 will not be used for any purpose other than those mentioned in this Clause 2.

3. RETENTION

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

b. All personal information collected under Clauses 1(b), 1(c), 1(d) and 1(e) will be retained on the mobile device for a period of 30 days from the date of collection after which, if it has not already been uploaded to the Server, will be purged from the App. All information collected under Clauses 1(b), 1(c), 1(d) and 1(e) and uploaded to the Server will, to the extent that such information relates to people who have not tested positive for COVID-19 will be purged from the Server 45 days after being uploaded. All information collected under 1(b), 1(c), 1(d) and 1(e)

of persons who have tested positive for COVID-19 will be purged from the Server 60 days after such persons have been declared cured of COVID-19.

c. Nothing set out herein shall apply to the anonymized, aggregated datasets generated by the personal data of registered users of the App or any reports, heat maps or other visualization created using such datasets. Nothing set out herein shall apply to medical reports, diagnoses or other medical information generated by medical professionals in the course of treatment.

4. RIGHTS

a. As registered user, you have the right to access your profile at any time to add, remove or modify any registration information that you have supplied.

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

5. DATA SECURITY

The App is equipped with standard security features to protect the confidentiality and security of your

information. Data is encrypted in transit as well as at rest. Personal information provided at the time of registration is encrypted before being uploaded to the cloud where it is stored in a secure encrypted server. Personal information that is stored in the Apps of other registered users that you come in contact with is securely encrypted and are incapable of being accessed by such user.

6. DISCLOSURES AND TRANSFER

Save as otherwise set out in Clause 2 with respect to information provided to persons carrying out medical and administrative interventions necessary in relation to COVID-19, no personal information collected by the App will disclosed or transferred to any third party.

7. GRIEVANCES

If you have any concerns or questions in relation to this Privacy Policy, you may address them to the Grievance Officer whose name and address are as follows: Mr. R.S. Mani, Deputy Director General (DDG) NIC (support.aarogyasetu@gov.in)."

(underlines supplied)

22. Thus, an individual who uses the *Aarogya Setu app* is to put to notice about the terms and conditions as well as the

privacy policy. The privacy policy contains the details under the following heads:

(a) Information collected and manner of collection;
(b) Use of information;
(c) Retention of information;
(d) Rights of registered user;
(e) Discloser and transfer.

Thus, *prima facie*, there is a notice to the users about the collection, use and retention of their individual information, as provided in paragraph 314.1 of the decision of the Apex Court in the case of ***Justice K.S. Puttaswamy*** (supra). A perusal of the documents produced at Annexures-R2 to R19 to the additional counter affidavit of the Government of India dated 10th December 2020 elaborately show the steps to be taken for installation of the app after it is downloaded. Step-4 gives choice of languages for installation of *Aarogya Setu app.* Step-5 questions the user whether he would like to kept informed if he/she has ever crossed paths with someone, who has been tested COVID-19 positive. He has to click 'next' and only thereafter he goes to step-6. The step-6 informs the user that Aarogya Setu app tracks through a Bluetooth and Location generated social graph, interaction of the person using the app

with someone who could have tested COVID-19 positive. The most important step is step-9 which calls upon the user to indicate his acceptance of the terms of use of service and Privacy Policy by clicking a button 'I agree'. Before he clicks 'I agree', by clicking on "terms of service" and "Privacy Policy", the user gets access to both the documents. The terms of service and Privacy Policy are available on the application itself. The user is put to the notice that the application monitors his device's proximity to another mobile devise. It also puts the user to notice that his data will be shared only with the Government of India and that the application does not allow his name and number to be disclosed to the public at large at any time. It is only after the user crosses the stage-9 by clicking the button 'I agree', he is required to upload further data like his cell phone number. Before clicking the said button, he is put to notice about the Privacy Policy which contains specific information regarding the use of the data uploaded for the purposes set out therein and its retention. At this stage, after reading the terms of use and privacy policy, the user has an option of opting out from the further process of installation. Step-14 gives the reasons why cell phone number of the user is required for contact tracing

and before going to further steps, the user has to click on the button 'I understand'. Before the user clicks/signs the button 'I understand', he is put to notice the purpose for which the mobile number will be used and the user is put to notice that the said mobile number will be used for contact tracing. Only after the user clicks on the button 'I understand', one time password (OTP) is generated and thereafter in step-16, he has to give his personal data i.e., his gender, name, age, profession and other details such as the countries travelled outside in the last 30 days, self assessment of the health etc. Thus, there is another option available to the person to opt out of the process of installation before he uploads his personal data.

23. Thus, a person who downloads and installs *Aarogya Setu app* is put to notice about the contents of the terms of service and Privacy Policy. He can download his personal data only after he is put to notice about the terms of service and Privacy Policy and the fact that his mobile number is required for contact tracing. He is put to adequate notice regarding the use of the data on the app for specific purposes, the transfer of the data to server, retention of the data etc., as set out in the privacy policy.

24. Thus, at this stage, when we are taking a *prima facie* view of the matter, we must hold that as the informed consent of the user is taken to Privacy Policy which contains the details about use of information, its transfer and retention, interim relief cannot be granted restraining the collection of information, the use of information and retention strictly as provided in the Privacy Policy which is available on the *Aarogya Setu app* itself. The reason is that *prima facie*, we have come to the conclusion that considering the procedure for installation of the *Aarogya Setu app,* there is an informed consent of the user taken for doing something which is permissible as per the Privacy Policy which is very much available on the *Aarogya Setu app.* In fact, before the user provides his personal mobile number and other details, his informed consent is required to be taken to privacy policy and the terms of service. He is given an option at two stages to opt out before sharing his cell phone number and other personal details.

25. Now, we come to what is provided in the said protocol regarding use and transfer of the personal data of the user. In the statement of objections, reliance is placed on the Order dated 11th May, 2020 issued by the Chairperson, Empowered

Group on Technology and Data Management by which, the said Protocol has been introduced. Paragraph-27 of the statement of objections is relevant which reads thus:

> "27. Averments in paragraph No.18 of the memorandum of writ petition, at the cost of repetition, it is reiterated that the Aarogya setu mobile application is one of the measures adopted for containing COVID-19 in the country, exercising the powers under the Disaster Management Act, 2005, read with Epidemic Diseases Act, 1897, National Disaster Management plan and Executive Powers, approved by the National Disaster Management Authority. It is submitted that under section 10 (2) (l) the National Executive Committee can lay-down guidelines, directions and the authorities regarding measures to be taken by them in response to the threatening disaster situation. Therefore, it is respectfully submitted that the implementation of the *Aarogya Setu app* is supported by law. In this connection Aarogya Setu data access and knowledge sharing protocol, 2020, was issued by the order dated 11/05/2020 of Chairperson, Empowered Group on Technology and Data Management. A copy of the same is produced and marked as **Annexure-R19.** As could be seen from the protocol, for the purpose of addressing the pandemic, NIC shall collect only

such response data as necessary. In the App, specific provisions are also made for maintaining the privacy of App Users. The data in the App are managed as per the said protocols. Here, data retention period of protocol has a Sunset Clause."

(underlines supplied)

26. We have perused the contents of Annexure-R19 which is an Order/Notification dated 11th May, 2020 regarding the issue of the said protocol. The said protocol is issued by the Chairperson, Empowered Group on Technology and Data Management appointed under Order dated 29th March, 2020 issued by the Ministry of Home Affairs, a copy of which produced as Annexure-R2. Clause-2 of Annexure-R2 is relevant which reads thus:

"2. The measures taken hitherto have been effective in containing the pandemic so far. However, considering the gravity and magnitude of the challenges, which are emerging with every passing day, there is a pressing need to augment and synchronies efforts cutting across various Ministries/Departments. Keeping in view the need for such comprehensive action and integrated response, in exercise of the powers conferred under the section 10 (2) (h) and (i) of the Disaster

> Management Act, 2005, the undersigned in the capacity as Chairperson, National Executive Committee, hereby constitute eleven Empowered Groups of Officers (as per Appendix). These Groups are empowered to identify problem areas and provide effective solutions therefor; delineate policy, formulate plans, strategize operations and take all necessary steps for effective and time-bound implementation of these plans/policies/ strategies/decisions in their respective areas."
>
> (underlines supplied)

27. On plain reading of clause-2 referred above, the role of the Empowered Group is of identification of problems/difficulties, finding out solutions, formulating contingency plan etc. There is nothing placed on record to show that the Chairperson, Empowered Group on Technology and Data Management is empowered to pass any order which will have a binding effect. *Prima facie*, it is not shown that this Empowered Group has any statutory power either under the said Act of 2005 or any other Act to pass such an order. There is nothing on record to show that the powers of the authorities under the said Act of 2005 have been delegated to the said Empowered Group. We have perused the said protocol. Clause 5(a) clearly stipulates that

any response data and the purpose for which it is collected by NIC shall be clearly specified in the Privacy Policy of Aarogya Setu App. Perusal of Privacy Policy available on the App. shows that there is no reference incorporated therein to collection of response data by NIC and purpose of collection. Clause 6 of the protocol permits sharing of data by NIC with the entities mentioned therein. The said entities are State Government, Public Health Institutions etc., But, the Privacy Policy says that the data will be shared only with the Government of India. Clause 8 permits NIC to share the response data for research purposes with third parties. It is pertinent to note that there is no reference to the said Clauses 5, 6 and 8 in the privacy policy or terms of service available on app itself. Thus, the collection of the data as per clause 5 and sharing of response data as per Clauses 6 and 8 is being done without the consent of the user, much less, an informed consent. Though Clause 8 provides for the anonymisation, there is nothing on record to show that the claim of anonymisation is tested by any agency. The sharing of health data of a citizen without his/her consent will necessarily infringe his/her right of privacy under Article 21 of the Constitution of India. Therefore,

prima facie, the said protocol regarding sharing of 'response data' cannot be permitted to be implemented for two reasons. Firstly, the user of *Aarogya Setu app* is not informed about the said protocol at all and the same is not at all a part of the terms of use or privacy policy which are available on *Aarogya Setu app* itself. The users are not even informed about the said protocol and the provisions therein about sharing of the response data before he uploads his personal information. Secondly, it is not the case made out by the Government of India that the informed consent of the user is obtained to sharing of the response data, as provided in the said protocol. The information contains data about the health of the user which all the more requires the protection of right to privacy. *Prima facie,* we find that the sharing and use of the response data as per the said protocol will infringe the right of privacy of the users, thereby amounting to violation of the rights guaranteed under Article 21 of the Constitution. We may note here that by order dated 10th November, 2020 which has been produced along with the memo dated 11th November, 2020, it has been directed that the said Protocol will remain in force for a further period of six months i.e., till 10th May, 2021.

28. Therefore, we pass the following interim order:

i) We accept the assurance given by the Government of India that no individual will be denied the benefits of any services that are being provided by the Governments, its agencies and instrumentalities on the ground that he has not downloaded and installed *Aarogya Setu app;*

ii) *Prima facie*, we hold that informed consent of the users of *Aarogya Setu app* is taken to what is provided in the privacy policy which is available on *Aarogya Setu app* itself and, therefore, there is an informed consent of the users of *Aarogya Setu app* which is limited only to collection and manner of collection of information, use of information and retention, as provided in the privacy policy which is available on the *Aarogya Setu app.* However, it is made clear that the use and retention of information and data shall remain confined to what is provided in the privacy policy which is available on the *Aarogya Setu app;*

iii) *Prima facie,* we hold that there is no informed consent of users of *Aarogya Setu app* taken for sharing of response data as provided in the *Aarogya Setu* Data Access and Knowledge Sharing Protocol, 2020, as there is no reference to the said protocol in the terms of use and Privacy Policy available on the app.

iv) Till further orders, we hereby restrain the Government of India and National Informatics Centre, the eighth and seventh respondents respectively from sharing the response data by applying the provisions of the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 issued vide order dated 11th May, 2020 (Annexure-R19) unless the informed consent of the users of *Aarogya Setu app* is taken;

v) However, it will be open for the Union of India and National Informatics Centre, the eighth and seventh respondents respectively to file an affidavit for satisfying the Court that the Chairperson, Empowered Group on Technology and Data

Management or the said Empowered Group is legally empowered to issue the said protocol and that the informed consent of the users of Aarogya Setu app is taken for implementation of clauses regarding sharing of the data as provided in the said protocol. After filing of an affidavit and the documents as aforesaid, it will be open for the said respondents to apply for vacating the limited interim relief granted as above, in terms of clause (iii).

Sd/-
CHIEF JUSTICE

Sd/-
JUDGE

Vr