IN THE HIGH COURT OF KARNATAKA AT BENGALURU

Writ Petition 7484 / 2020 (GM-PIL)

Between:

Mr Anivar A Aravind …Petitioner

And

Ministry of Home Affairs & Ors …Respondents

Submissions of the Petitioner

for Stay on the Operation of the Aarogya Setu App

Contrary to Puttaswamy 1

1. This is an app which is compulsory and which invades privacy ostensibly for the greater good. In so far as there is no law enacted for the invasion of privacy, the app is constitutionally invalid and cannot be allowed to continue. The app must be stayed with immediate effect. (2017 10 SCC 1 at page 509).

Mandatory or not?

2. The use of the app is said to be mandatory (p.46). A subsequent guideline dated 17.05.2020 seems to indicate that it is not and that "best effort basis" should be attempted (page 53). Therefore,

government should immediately clarify as to whether it is mandatory or voluntary. The Railways and Airlines have declared the app to be mandatory (pp. 83, 91, 94, 98, 106).

Terms of Service

3. The Terms of Service, Annexed A hereto, at Clause 6 dealing with 'Liability', specifically states that government would not be liable for the failure of the app and other failures in the functioning of the app. This violates the principle of accountability. The app is therefore arbitrary in its design and operation. Clause 7 similarly violates the accountability requirement and provides no warranty of fitness and is therefore arbitrary.

4. Clause 2 makes mandatory the use of GPS services which is never done anywhere in the world, and not followed even by google Google and Apple. The use of GPS services makes the app overbroad, hazardous and renders the collection and use of data excessive. All countries in the developed world use Bluetooth alone and this serves the purpose of warning the app user that steps ought to be taken to be tested and treated. So far so good. The GPS services expand the area of intrusion enormously in that the quality of data is so poor that persons far apart are virtually shown as proximate to each other, thus, making the app meaningless. The tracking of persons at 15 minute interval is insidiously designed to

identify and pick up persons who are thought to be positive and to force them into a regime of treatment and quarantine against their will. The use of the GPS is therefore contrary to the principle of data minimisation (2019 1 SCC 1, p.347)

5. Persons using the app could in all probability trigger false positives on a large scale given the population density, fleeting and passing movements will trigger orange and red responses in the app on a large scale even though the persons using the app may not be affected at all.

6. The prohibition on sharing devices is arbitrary and intrusive because in poorer families the entire family may be using one mobile device. Moreover, mandatory requirement of keeping both Bluetooth and GPS on at all times drains battery and causes grave inconvenience.

Privacy Policy

7. The Privacy Policy, Annexure B hereto, is unfair and arbitrary in that it permits the State to revise the policy from time to time without taking the consent of the user of the app each time the policy is revised.

8. The continuous monitoring of the location of the user is pernicious as it is a huge invasion of privacy which is not justified by any law, let alone a valid law, and the ultimate purpose is to use the app to

swoop down on unsuspecting app users and to force them into quarantine centres or for compulsory medication. This is contrary to the use of such applications elsewhere in the world where monitoring is not done and the app is specifically used only to warn of the possibility of some contact and acts as an advisory to take precautionary steps and nothing more.

9. The app as used at the moment, particularly for slum areas and other places where population densities are high, are capable of multiple false positives followed by large scale intrusion and punitive action by the State. The Brookings Institute document at page 79 points that people have an average of a dozen close contacts a day nevertheless infected persons transmit only two or three people throughout the entire course of the disease. In the privacy policy however the consequences of a false positive would result in compulsory medical and administrative interventions by the State. Further, though the Privacy Policy gives the impression that the data collected would be purged within a specified period, Clause 3 relating to 'Retention' shows that the data is retained for a much longer and indeterminate period of time.

10. The purposes of data collection is much wider than the use internationally where it is limited to cautioning persons to perhaps take action if the app turn from green to orange or red. The Indian version expands the scope to very close monitoring and collection

of data, compulsory medication, compulsory quarantine and other punitive measures. This is contrary to the principle of Purpose Limitation which is set out in 2019 1 SCC 1 at p.350.

11. The Terms of Service and Privacy Policy contains loopholes which allow for unreasonable and indefinite periods for retention of data, and, therefore, this is contrary to the principle of Time Period for Data Retention as set out in 2019 1 SCC 1 at p.351.

Data Access and Knowledge Sharing Protocol

12. The protocol dated 11.05.2020 (p.60) enabling data access and knowledge sharing is unconstitutional because there is no law enacted for the purpose. The power to be exercised by the Empowered Group on Technology and Data Management requires legislative backup. In the absence of this no person can engage in granting access and sharing data.

Justice BN Srikrishna's observations

13. The Hon Former Judge of the Supreme Court commented on the app stating that in the absence of a Personal Data Protection law, the Aarogya Setu app is utterly illegal (Annexure C hereto).

MIT Technology Review

14. At Annexure D hereto, the MIT Tech Review found lack of transparency, absence of limitations on how the data is used, provisions for destructions of data after a period of time, data collection not minimised as required, and other flaws.

Joint Statement on Contact Tracing

15. Page 69 of the petition sets out the joint statement which defines the situation as one of unprecedented surveillance. The GPS system is criticised for lacking accuracy and also because the data is sent to a centralised location in India whereas abroad it is sent to a decentralised location. The European Parliament has decided overwhelmingly for a decentralised approach, and the voluntary use of contact tracing apps.

Discrimination against the Poor and Disabled

16. Since, only 35% of the population have smartphones the poor are excluded and the app becomes ineffective since the overwhelming majority do not have such phones. The blind, the deaf and the other disabled sections are also discriminated against does not have accessibility features such as high contrast, audio prompts and screen readers, etc.

Bangaluru, 04.06.2020 Siddharth Baburao, Adv for the Petitioner

Annexure A

TERMS OF SERVICE (Aarogya Setu App)

These terms of service (Terms) govern your use of the Aarogya Setu application for mobile and handheld devices (App) and the services provided thereunder. Please read these terms and conditions (Terms) carefully before you download, install or use the App. By clicking on the "I Agree" button, you signify your acceptance of the Terms, and your agreement to be bound by them. The Terms may be amended from time to time with notice to you. In order to continue using the App, you will be required to accept the revised Terms.

1. SERVICE OVERVIEW

The App is part of a service designed to (i) enable registered users who have come in contact with other registered users who have tested positive for the severe acute respiratory syndrome Coronavirus 2 (COVID-19) to be notified, traced and suitably supported, (ii) to function as an indication of whether or not a user has been infected or is likely to have been infected. (iii) provide users useful information in relation to COVID-19, (iv) to allow users to access convenience services in relation to COVID-19, and (v) to display a government issued ePass (Services). When the App is installed on your mobile or handheld device,

it detects when your device comes within Bluetooth range of any other registered user's device and initiates a protocol by which the information specified in the Privacy Policy (including location information) about that other registered user is collected. In the event you test positive for COVID-19, the Government of India will contact and/or inform such registered users you have come in contact with over the past 30 days who have a risk of being infected, to administer the appropriate medical intervention. Similarly, you will be notified if, as a result of having come in contact with any persons who have tested positive for COVID-19, that you have a risk of being infected. The App also allows users to conduct a self-assessment test to assess whether their symptoms combined with other relevant factors affects their risk of being infected. The App will also serve as digital representation of an e-Pass where available. The App will also provide links to convenience services offered by various service providers. Accessing the links will take users to external sites from where these convenience services will be provided.

2. REQUIREMENTS FOR USE

You agree to turn on and allow the App access to the Bluetooth and GPS services on your mobile or handheld device. You acknowledge that if your device is switched off or in airplane mode, if Bluetooth and GPS services on your device are turned off or if you revoke the App's access to Bluetooth and GPS services on your device, it will not be able capture

all necessary information which will impair the completeness and accuracy of the Services. You agree to keep the mobile or handheld device on which the App is installed in your possession at all times and to not share it with or allow anyone else to use it. You acknowledge that if you do so it could result in you being falsely assessed as likely to infected with COVID-19 or not being assessed as such when you are.

3. USE

You agree that you will only use the App in good faith and will not provide false or misleading information about yourself or your infection status. You agree that you will not do anything to throttle, engineer a denial of service, or in any other manner impair the performance or functionality of the App. You agree that you will not use the App for any purpose for which it was not intended including, but not limited to, accessing information about registered users stored in the App, identifying or attempting to identify other registered users or gaining or attempting to gain access to the cloud database of the Service.

4. PRIVACY

You hereby consent to the collection and use of your personal information for the provision of the Services. The details of the personal information collected and the manner in which it collected and Draft

Version by whom as well as the purposes for which it will be used is more fully set out in our privacy policy which is available here. You are free to choose not to provide this information at any time by revoking the App's access to Bluetooth and GPS services. You can also delete the App from your mobile or handheld device, however, should you do so, you acknowledge that you will no longer be able to avail of the Services.

5. DISRUPTION

You agree that you have no expectation of, or right to permanent and uninterrupted access to the Services. While the Services are intended to be accessible to you from everywhere on a 24x7 basis, from time to time and without prior notice of downtime, access to the App or the Services or to any part thereof may be suspended on either a temporary or permanent basis and either with respect to all or a certain class of users.

6. LIABILITY

The Government of India will make best efforts to ensure that the App and the Services perform as described but will not be liable for (a) the failure of the App or the Services to accurately identify persons in your proximity who have tested positive to COVID-19; (b) the accuracy of the information provided by the App or the Services as to whether the

persons you have come in contact with in fact been infected by COVID-19.

7. DISCLAIMER

The App is being made available on an "as-is" basis. All services such as those provided by this App are never wholly free from defects, errors and bugs, and the Government of India provides no warranty or representation to that effect or that the App will be compatible with any application, or software not specifically identified as compatible. The Government of India specifically disclaims any implied warranties of fitness for a particular purpose or non-infringement. The functioning of the App is dependent on the compliance by all registered users of the App with these Terms. Accordingly, the Government of India disclaims all liability on account of such non-compliance by other registered users. The Services that are being provided (including the self-assessment test, its results and any notifications sent by the App) are not a substitute for common prudence, medical diagnosis, or specific therapeutic and epidemiological measures necessary to combat COVID-19.

8. DEFECT REPORTING

You can report any defects or bugs in the App or the Services to support.aarogyasetu@gov.in. The Government of India will make every endeavour to address all reported bugs and defects.

9. GOVERNING LAW

These Terms shall be governed by the laws of India.

(True Copy)

Annexure B

PRIVACY POLICY (Aarogya Setu App)

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 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 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 Clauses 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 visualisations 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(c) 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 sanitised 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 Clauses 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 a 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)

(True Copy)

Annexure C

Mandating use of Aarogya Setu app illegal, says Justice B N Srikrishna: Justice Srikrishna said that the guidelines cannot be considered as having sufficient legal backing to make the use of Aarogya Setu mandatory.

Written by Apurva Vishwanath | New Delhi | Updated: May 13, 2020 11:37:10 am

On May 1, the Ministry of Home Affairs, in its guidelines after the nationwide lockdown was extended, made Aarogya Setu App mandatory for employees of private and public sector offices. It also asked local authorities to ensure 100% coverage of the app in containment zones. The guidelines were issued by the National Executive Committee set up under the National Disaster Management Act (NDMA), 2005.

The Noida police then said that not having the Aarogya Setu application would be punishable with imprisonment up to six months or fine up to Rs 1,000.

Former Supreme Court Judge B N Srikrishna, who chaired the committee that came out with the first draft of the Personal Data Protection Bill, termed the government's push mandating the use of Aarogya Setu app "utterly illegal".

"Under what law do you mandate it on anyone? So far it is not backed by any law," the former judge told The Indian Express.

"The Noida police order is totally unlawful. I am assuming this is still a democratic country and such orders can be challenged in court," he said.

Justice Srikrishna said that the guidelines cannot be considered as having sufficient legal backing to make the use of Aarogya Setu mandatory. "These pieces of legislation — both the National Disaster Management Act and Epidemic Diseases Act — are for a specific reason. The national executive committee in my view is not a statutory body," he said.

In July 2017, while the Supreme Court was still examining whether the right to privacy would constitute a fundamental right, the government had appointed Justice Srikrishna to head the committee on data protection. The committee of experts and officials held public hearings across the country and submitted a report in July 2018, in which it also proposed a draft data protection law. The Bill is yet to be brought to Parliament for approval. The report recommended that "processing of personal data must only be done for clear, specific and lawful" purposes. The committee recommended several rights for the data principal (whose personal data is collected) – from revoking consent granted for processing data, notifying a breach to having their incorrectly processed data rectified by the authorities.

The Supreme Court in the landmark 2017 ruling that recognised the fundamental right to privacy laid down a three-fold test to examine constitutionality of government actions that could invade a citizen's right

to privacy. The first condition is that the action taken must be under a law duly passed by Parliament and the government will have to show it had a "legitimate state interest" to violate the right to privacy apart from having considered all less intrusive measures before violating the right.

On Monday, the Aarogya Setu Data Access and Knowledge Sharing protocol was issued, setting up principles for collecting and processing of data. The protocol is an "order" by the Empowered Group on Technology and Data Management set up by the National Executive of the Disaster Management Act.

Justice Srikrishna said that the protocol would not be adequate to protect the data. "It is akin to an inter-departmental circular. It is good that they are keeping with the principles of the Personal Data Protection Bill but who will be responsible if there is a breach? It does not say who should be notified," he said.

In a webinar organised on Monday by Daksha Fellowship, a legal education group, he called the new protocol a "patchwork" that will "cause more concern to citizens than benefit."

"It is highly objectionable that such an order is issued at an executive level. Such an order has to be backed by Parliamentary legislation, which will authorise the government to issue such an order," said Justice Srikrishna.

"If it is traced to NDMA, the NDMA has no provision for constitution of an empowered group. (Under) what provision of law is this order issued?

I cannot understand … If there is a breach of data here, who is answerable, what action has to be taken and (who is) accountable for the data breach. This should really have been traced ideally to PDP (Personal Data Protection) or through NDMA by an appropriate amendment," he said.

— with inputs from Aashish Aryan

(True Copy)

Annexure D

India forcing people to use its covid app, unlike any other democracy

Millions of Indians have no choice but to download the country's tracking technology if they want to keep their jobs or avoid reprisals.

by Patrick Howell O'Neill May 7, 2020

The world has never seen anything quite like Aarogya Setu. Two months ago, India's app for coronavirus contact tracing didn't exist; now it has nearly 100 million users. Prime Minister Narendra Modi boosted it on release by urging every one of the country's 1.3 billion people to download it, and the result was that within two weeks of launch it became the fastest app ever to reach 50 million downloads.

"We beat Pokémon Go," says a smiling Arnab Kumar, who is leading development of the service for the Indian government.

But although the app's growth is unprecedented, it is extraordinary in an even more important way: if you don't install it, you might lose your job, get fined, or go to jail.

India is currently the only democratic nation in the world that is making its coronavirus tracking app mandatory for millions of people, according to MIT Technology Review's Covid Tracing Tracker, a database of global contact tracing apps.

While official policy is that downloading the app is voluntary, the truth is that government employees are required to use it, while major private employers and landlords are mandating it as well. The city of Noida is now reportedly fining and even threatening to arrest anyone who fails to install the app on their phone.

It's a dramatic step generating fierce criticism from civil liberties experts nationally, and from all over the globe.

Rahul Gandhi, a prominent member of the Indian parliament and former leader of the opposition Indian National Congress, is among those who have criticized the app, charging that it has "no institutional oversight" and raises "serious data security and privacy concerns."

"Technology can help keep us safe," Gandhi recently tweeted. "But fear must not be leveraged to track citizens without their consent."

"There is an infringement on human rights that is not justified here," says Estelle Massé, a senior policy analyst at the digital rights group Access Now. "There is a risk of initiating a tool that can be repurposed for surveillance after the pandemic."

A massive all-in-one undertaking

MIT Technology Review's database shows that India's app is unique in a number of other ways, too. Many countries are developing limited services that use Bluetooth or GPS to give "exposure notifications" to

people who have interacted with someone found to have covid-19. India's app, though, is a massive all-in-one undertaking that far exceeds what most other countries are building. It tracks Bluetooth contact events and location—as many other apps do—but also gives each user a color-coded badge showing infection risk. And on top of this, Aarogya Setu (which means "a bridge to health" in Hindi) also offers access to telemedicine, an e-pharmacy, and diagnostic services. It's whitelisted by all Indian telecom companies, so using it does not count against mobile data limits.

What the app lacks also sets it apart. India has no national data privacy law, and it's not clear who has access to data from the app and in what situations. There are no strong, transparent policy or design limitations on accessing or using the data at this point. The list of developers, largely made up of private-sector volunteers, is not entirely public.

Kumar stresses that the app was built to the standards of a draft data privacy bill that is currently in the country's parliament, and says access to the data it collects is strictly controlled. But critics have expressed concern because it is not open source, despite an Indian government mandate that its apps make their code available to the public. Kumar says that this is a goal for Aarogya Setu and will happen down the line, but he could not confirm a timeline or expected date.

When Aarogya Setu was first announced, the Indian government did seek consent, and using the app initially sounded voluntary. Today, at

least 1 million people have been given orders to use it, including central government workers and employees of private companies like the food delivery services Zomato and Swiggy. It's a well-practiced tactic in India, where "voluntary mandatory" technology has a history of being used as a gatekeeper to certain important rights.

While India is the only democracy to make its contact tracing app mandatory for millions of people, other democracies have struck deals with mobile phone companies to access location data from residents. In Europe, the data has largely been aggregated and anonymized. In Israel, law enforcement focused on the pandemic has used a phone tracking database normally reserved for counterterrorism purposes. The Israeli government's tactics have been the subject of a legal battle that made its way up to the country's Supreme Court and legislature.

Not transparent

Many of these difficulties can be traced to a lack of transparency. Neither the privacy policy nor the terms of service for the app were publicly accessible at the time of publication, and the developers have not shared them despite requests. Since the app is not open source, its code and methods can't easily be reviewed by third parties, and there is no public sunset clause stating when the app will cease to be mandatory, although Kumar says data is deleted on a rolling basis after, at most, 60 days for sick individuals and 30 days for healthy people. And there is no clear

road map for how far India's national and state governments will go: one recent report said the government wants Aarogya Setu preinstalled on all new smartphones; another said the app may soon be required to travel.

In the early days of the app's development, Kumar said it would leverage the technology being jointly developed by Apple and Google for iPhone and Android. That system will be released in just a few days, but it now comes with rules that include requiring user consent and banning location tracking—neither of which Aarogya Setu complies with. Kumar says Google engineers have been in close contact with Aarogya Setu's developers, and his team will evaluate whether they can still implement the decentralized Silicon Valley system, which is intended to preserve privacy. Google and Apple have fast-tracked the app into both the Android and iOS app stores.

But there are still deep concerns that blurring the line between voluntary and mandatory, and between privacy-preserving and privacy-invading, will have long-term consequences.

"There is no effort made by the state to earn citizen trust," says Anivar Aravind, executive director at the civic-technology organization Indic Project. "Here are a set of private-sector corporate volunteers, with no accountability, that built an app for governments that is forced to personal devices of everyone."

(True Copy)