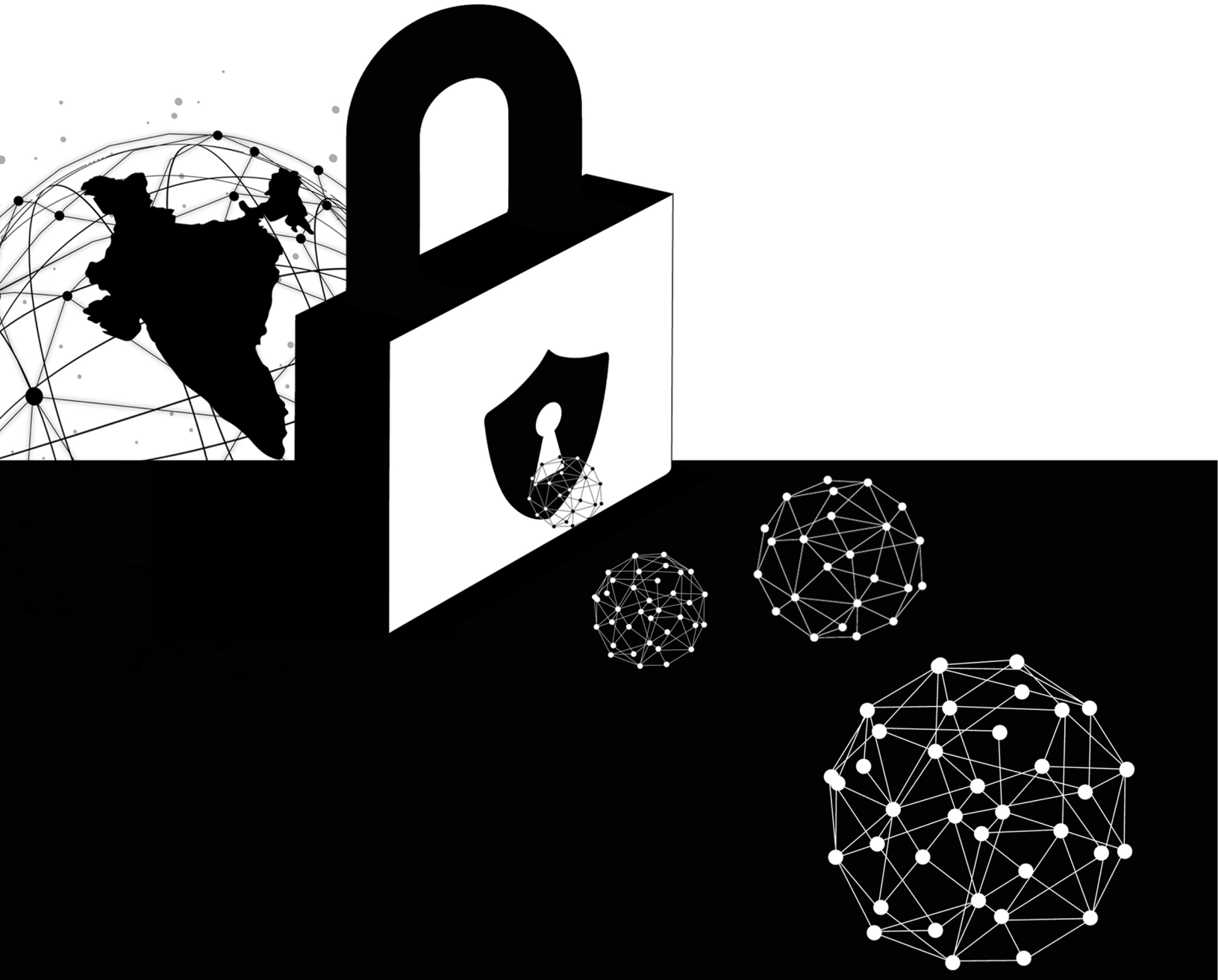
The Dialogue

Inform Engage Ideate



PRIVACY FRAMEWORK
FOR THE AAROGYA SETU APP

Privacy Framework for the Aarogya Setu App

"Life is like the harp string, if it is strung too tight it won't play, if it is too loose it hangs, the tension that produces the beautiful sound lies in the middle." - Gautam Buddha

Authors

Pranav Bhaskar Tiwari[1], Ayush Tripathi[2], Harsh Bajpai[3], Karthik Venkatesh[4], Arya Tripathy[5] & Kazim Rizvi[6].

[1] Policy Research Associate, The Dialogue
[2] Policy Research Associate, The Dialogue
[3] Research Scholar, Durham University
[4] Strategic Engagement and Research Fellow, The Dialogue
[5] Principal Associate, Priti Suri & Associates
[6] Founding Director, The Dialogue

Index

Executive Summary

Technology is one of the tools in the fight against the pandemic and Governments around the world have been deploying technological solutions to tackle the threat posed by COVID-19. While Singapore has launched TraceTogether, Australia has come out with COVIDSafe for developing a contact tracing system. Working towards a similar goal, the Indian Government has launched a contact tracing application called 'Aarogya Setu'. The App collects personal information and location data to track individuals who have either tested positive for COVID-19 or have come in contact with a positive case. While downloading this application software was voluntary to begin with, the Government of India *vide* order dated 1st May 2020 made it mandatory to download this app in private and public offices as well as in the containment zones. Though the App can be a useful tool in containing the outbreak, a few tweaks and evolutions in the privacy policy can make the app much more robust, it will enhance its privacy and make it more secure.

Legal Challenges and Way Forward

Firstly, the app does not have any legal standing of its own. Neither an Ordinance, nor an Act has been passed by the President or the Parliament respectively to give a legal foothold to this application. The *Puttaswamy* judgement mandates that the right to privacy may only be curtailed per a law which has a legitimate purpose. The same has not been adhered to in the present circumstance.

Secondly, the privacy judgement has laid down three key tests for the measures that abridge privacy i.e. Necessity, Proportionality and Legality. The measures taken must harmonise with the right to privacy and should limit themselves to the extent necessary and proportional, in order to meet the ends of maintaining public health. This framework suggests that the measures that could be taken to ensure that the application is within the bounds of privacy judgement. Moreover, without a data protection law in our country, it is necessary that utmost caution be taken to adhere to privacy principles.

Privacy Challenges and Way Forward

The privacy policy of the Aarogya Setu app has a few shortcomings. *Firstly*, the lack of transparency and verifiability raises many concerns with regard to its operation. It is important that to popularise it among the masses, the application be open source. Moreover, by allowing data auditing, concerns regarding lack of checks and balances, and accountability will be resolved.

Secondly, the app does not clearly define the purpose of its use. It is important that the privacy policy clearly mentions the purpose of the app and specifically denies any other kind of use. Further, the policy should be designed in such a way that minimal data is collected for maximum output.

Thirdly, the privacy policy suggests that the data will be anonymised but does not talk about the techniques that will be used for anonymisation. Given the fact that cryptography has reached a level where we can conceivably deanonymize a wide variety of encrypted data, it is important that technologies used for anonymisation must have an in-built privacy and security architecture that is auditable.

Fourthly, The current time frame for storage of data is 30 days on mobile, 45 days on server if the patient has tested negative but has come in contact with an infected person, and 60 days in case patient has tested positive, from the date of uploading on the server. The limit for storing personal data should be fixed at 21 days. It is important that the data be stored for a lesser period to prevent any misuse and external interference. Further, privacy policy must have a sunset clause to prescribe that anonymised data sets will be purged from the servers.

Fifthly, though the privacy policy states that data will not be shared with anyone except the health officials, it does not disclose the sharing protocol. Additionally, the privacy policy must be clear on which departments within Government of India will have access to data, to ensure purpose limitation that will minimise the risk of associated misuse.

Recommendations

1. Bring out an ordinance to establish a legal standing for the application.
2. The application should only be made mandatory to download in the containment zones.
3. The application must be made open source for the sake of transparency and inspiring public confidence.
4. The Government should allow independent data auditing to ensure check and balance and attribute accountability.
5. Techniques that will be used for anonymisation should be disclosed.
6. The time frame for storage of data should be reduced to 21 days. If the Government deems fit that it needs to be kept for the stated duration, a reason should be provided for the same.
7. The Government should clearly state the purpose for which anonymised data will be used and specifically deny any other purpose. The data should not be used for any other purpose except for research, academics and statistics.
8. A sunset clause should be provided in the privacy policy after which all the data. Personal or anonymised or should be purged from the servers.
9. In the absence of data protection authority, a grievance redressal forum must be made under judicial oversight in order to address any issues and concerns arising out of the application software. Further, the Government should assume civil liability for any misidentification of a person through this application.
10. Restrict the access to this data only to concerned ministries and departments.
11. In the absence of a data protection law, the parameters of necessity, proportionality and legality must be observed at every level and stage of this app. A judicial committee composed of former supreme court judges should be constituted to ensure that these parameters are being adhered.

Analogy with Popular Culture

In the critically acclaimed movie 'The Dark Knight', the protagonist Batman, in his quest to catch and apprehend the villain, The Joker, builds a machine that enables surveillance of the entire city of Gotham using a specific technology that tracks the movement of people in real time. His colleague, after getting introduced to the machine, expresses his deep concern over the privacy and security challenges associated with the technology. Their conversation builds up to question the need of the machine and the high cost to privacy, and whether the machine is worth this cost.

The protagonist, while respecting the concern, also demonstrates the need to deploy the machine, since the villain was an extremely clever and intelligent opponent. Finally, in order to catch him, Batman resorts to this extreme step. Privacy was built into the machine, which was encrypted, and could be operated and destroyed only by his colleague, Mr. Lucious Fox, once the job was done (purpose limitation). Moreover, while Mr. Fox agrees to help the protagonist by operating the machine for him, he also simultaneously offers his resignation if the technology continues to stay post the apprehension of the villain.

Consequently, the machine was destroyed by Mr. Fox at the end of the movie after Batman was able to catch his nemesis, and it was only logical that the narration in the background states that it was important to reward the faith of the people.

1. Background

For the first time since independence, India finds itself in the state of a Public Health Emergency. The COVID-19 pandemic has attacked countries worldwide and fractured the burgeoning health infrastructures globally and is now threatening to spill-over into a socio-economic disaster. India is no exception to this phenomenon that has rapidly taken over the ability of nations to continue as if it's 'business as usual'. This is forcing unprecedented measures that have never been seen before - lockdowns leading to a complete economic shutdown. The Novel Coronavirus, as it is known, is unlike any other outbreak in the recent past, as it is notorious for the high rate of spread, long incubation periods (upto 14 days) and without any vaccine. This potent combination makes it an 'invisible enemy' that, within a very short span of time, has derailed economies worldwide. India might be staring at a 'contraction' (negative growth) for the first time since 1980. If not controlled within the next couple of months, India could witness a significant job loss that could take upto two years to bring back normalcy. The policy response therefore must take into account maximum resource allocation that is aggressive, implementable and timely in nature. Presently, nothing is more critical than containing the spread of the virus as the country is literally in an 'ICU'.

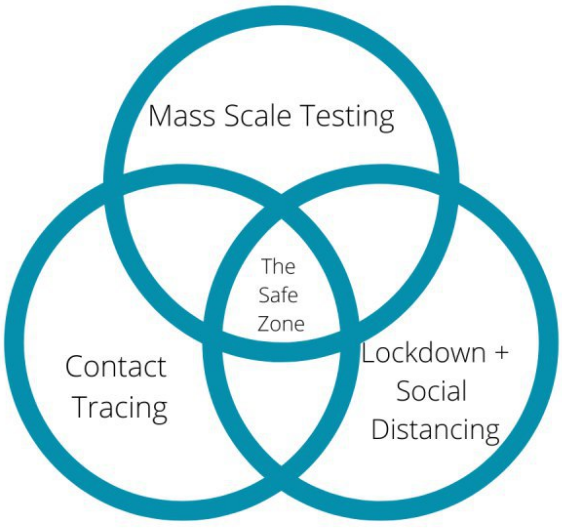


Figure 1.0

The methods that are being deployed globally to 'flatten the curve' can be summed up into the following mechanisms:

1. Contact Tracing
2. Lockdown followed by Social Distancing
3. Nationwide Testing

Practicing social distancing and enabling proper testing through contact-tracing apps will reduce transmission of virus, avoid increased morbidity and thereby decrease the pressure on the health system. To achieve success, all three methods have to be deployed simultaneously to cast the widest net possible on the spread of the virus. As depicted in Figure 1.0, the 'safe zone' is the ideal place to be, where people are practicing social distancing, are being tested and use contact tracing to keep themselves informed.

1.1 COVID-19 Pandemic - A Socio-Economic Challenge

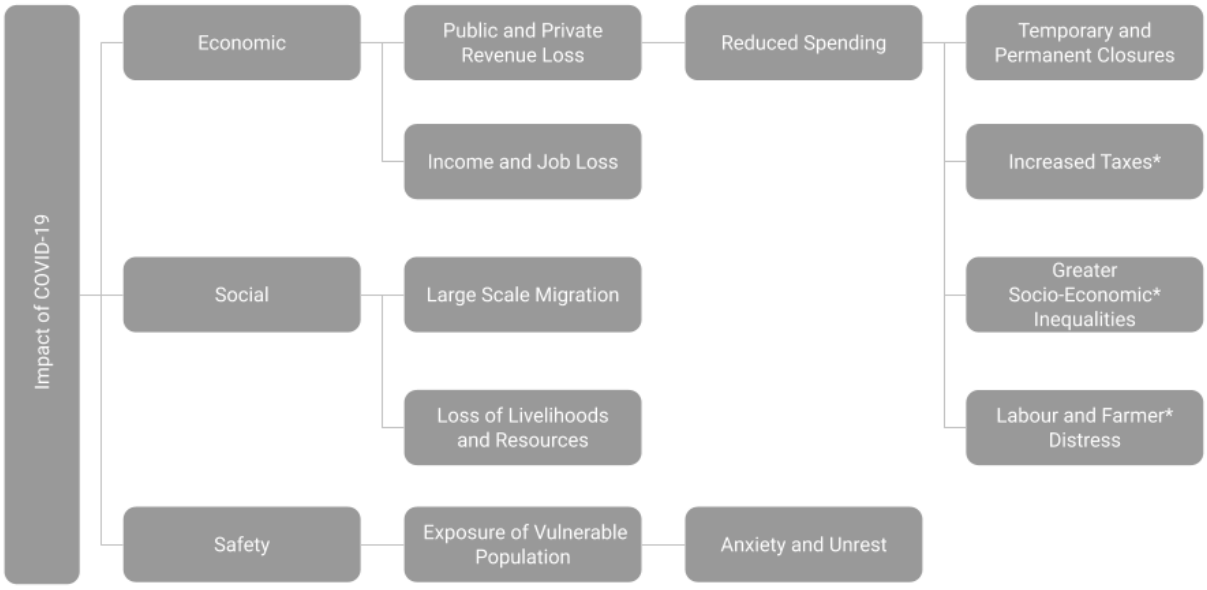


Figure 2.0

What started as a public health emergency has soon culminated into an economic crisis that will need the best of India's talent and might to overcome in the coming months. While the first case was reported by the end of January, it was only in late February and early March that the pandemic arrived. As the nation was sent into a lockdown since 24th March, India's economy since took a downturn, as April was marred by one of the lowest ever spending patterns and tax revenues recorded in recent history. While the virus moved and spread at racing speed, the low economic output has now threatened temporary and permanent closures of businesses that have put hundreds of millions of jobs at stake. A revival to the pre-covid growth is a distant dream for now and a strong policy response strategy with increased spending is critical to ensure that prices of commodities do not shoot up in the coming weeks. The loss of present and future economic opportunities to the working-class population has led to large scale migration and loss of resources to live, compounded with an uncertain future. This can also potentially weaken governance structures and can cause unrest. In Figure 2.0 the authors demonstrate various consequences from the spread of the virus on communities and people which will have lasting socio-economic impact for some time to come.

1.2 Technology as a resource to combat the outbreak

Pandemics and outbreaks have occurred throughout the history of mankind and until recently it was a massive challenge to comprehensively understand the origin, cause and nature of the spread. Contrasted with that, today, contact tracing systems have emerged as a potentially viable tool, amongst other mechanisms, to fight the pandemic. Contact tracing means identifying all the recent interactions of infected individuals to determine whom they might have infected. Progress in digital technology has perhaps never been more evident than in this moment of widespread social distancing measures. The widespread rollout of testing to a large population, which caught community transmission only through these apps has been crucial to the South Korea success story.

During the Ebola outbreak, the Government had to rely on human interviews due to lack of mobile penetration. Infected patients were asked to list recent interactions with family, friends, family, relatives and businesses. However, the effectiveness of such an exercise was always in question as humans have faulty memories that raised questions on the chances of its success.

Further, person-to-person interviews are slow and cannot work in situations where the rate of infection is so high that it doubles every ten to fourteen days. For a successful tracing mechanism, contact tracing cellphones and smartphones are a handy tool that can log human activity. It's faster, more accurate and effective.

Such applications become even more relevant when people start resuming daily routines and contact tracing will be critical to contain new coronavirus infection clusters. Without these efforts, the virus could propagate unnoticed which can prevent policy makers from seeing the complete picture, and that could result in further lockdowns in the future.

1.3 The importance of Citizen's Participation - A Fundamental Duty to protect our Communities

In a pioneering move, the Aurangabad bench of the Bombay High Court initiated suo-moto public interest litigation after taking cognizance of certain news reports highlighting the plight of migrant workers who were headed to their hometown in Madhya Pradesh. After hearing the submissions from the State regarding the facilities provided, the Court appreciated the efforts of the Aurangabad administration, NGOs and volunteers in creating awareness and observed,"[W]hile this court expects effective measures from the respondent state authorities and corporation, it also expects that citizens would remind themselves fundamental duties and would discharge them to deal with the outbreak of Covid-19 pandemic."[7] Article 51-A of the Indian Constitution obliges citizens to promote harmony and spirit of common brotherhood among all people of India. Solidarity is an attitude of a community that initiates participation and fosters the realization of the common good.

[7] The Registrar Judicial High Court of Judicature at Bombay Bench at Aurangabad v/s The State of Maharashtra and Others Aurangabad (Civil)SMPIL/10541/2020. *See also* Press Trust of India (2020), Citizens Should Remember Fundamental Duties Amid Pandemic: HC, Deccan Herald, Retrieved from https://www.deccanherald.com/national/citizens-should-remember-fundamental-duties-amid-pandemic-hc-823603.html

Social distancing is social solidarity for the present times. An empathetic response based on the recognition of mutual needs and shared identity is the need of the hour. Even the International rules like UN Siracusa Principles agree that restrictions can be placed on freedom of movement within a nation at times like COVID-19, on account of protecting national security, or the rights and freedoms of others (like, the Right to Health of others).

1.4 Aarogya Setu

The Aarogya Setu App is the balancing act wherein technology is deployed in the fight against the pandemic. It traces citizens who are under risk of contracting COVID-19 based on contact, helps to understand the nature of spread, identify hotspots to improve policy decisions. As the Government decides to open the economy gradually, real time response mechanisms require real time insights. As the app works on collecting and processing 'personally identifiable information', the right to privacy as guaranteed under the Constitution gets invoked. Responding to a public health emergency may require the Government to collect and process personal data, but any such processing for targeted surveillance mechanisms must be reasonable, necessary and proportionate. There are also indications from other countries that self-imposed restrictions do not always work out. That being said, the State is bound to take affirmative action towards protecting public health, and community interests at large, to flatten the curve. The fight against the pandemic cannot be completely reliant on Union and State Governments, since a lot of it is dependent on active participation by the citizenry. It is towards this end that technological solutions that are people centric are deployed. To prevent sustained human-to-human transmission, a system that involves rapid data collection, analysis, assessment and timely reporting is key.

1.5 Harmonisation of Right to Health and Right to Privacy

As per the Lockean Social Contract, protecting the life of its citizens is the prime responsibility of the State. The Constitution guarantees this right to all. The *right to health* is a facet of the *right to life* under article 21 of the Indian Constitution. It also guarantees the *right to privacy* of an individual. However, when the two rights are in conflict it is critical to ensure a harmonious

construction. The two rights need to be weighed in the balance, to ensure that the least amount of infringement is caused cumulatively[8].

1.6 Proportionality at the heart of Reasonable Restrictions

Drawing from earlier pandemics such as SARS, Ebola etc., the global community is increasingly relying on science, technology and data driven policies. Aggregated health datasets from across the world can be useful in research and help in understanding the clinical, epidemiologic, and molecular features of an infectious disease.

These circumstances allow the imposition of *'reasonable restrictions'* on the right to freedom of movement and privacy. Even while imposing such restrictions, the State has the onus to follow the principles laid out in the Puttaswamy Judgement[9] which is popularly known as the *"Right to Privacy"* judgement. The Proportionality test laid down by the Supreme Court in Puttaswamy for deciding whether a restriction of right to privacy is reasonable or not has four prongs:

- Legality (requirement of a law, with a legitimate purpose);
- Suitability (the Government's action must be suitable for addressing the problem, i.e., there must be a rational relationship between means and ends);
- Necessity (i.e., it must be the least restrictive alternative), and;
- Proportionality *stricto sensu* (there must be a balance between the extent to which rights are infringed and the State's legitimate purpose).[10]

[8] Central Public Information Officer, Supreme Court Of India v Subhash Chandra Agarwal, Civil Appeal No. 10044 of 2010.
[9] Justice K.S.Puttaswamy (Retd) v. Union Of India And Ors. (2017) 10 SCC 1.
[10] Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. IndraStra Global, 11, 1-5, Retrieved from: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2, *See also:* Bhatia, Gautam., (2020). Legal Flaws On The Mandatory Imposition Of Aarogya Setu App. LiveLaw.in, Retrieved from: https://www.livelaw.in/columns/coronavirus-and-the-constitution-xxi-the-mandatory-imposition-of-the-aarogya-setu-app-156134.

A balance must be struck between confidentiality of information of the individual, privacy and data protection concerns, and benefit for the community at large. *While the downloading of the App was voluntary to begin with, it has now been made mandatory for all living in identified containment zones, for government employees, and for those working in the private sector (attending office).* To prevent the Aarogya Setu App from becoming a tool for mass surveillance, this paper proposes a privacy respecting 'Proportionality Framework' and suggests measures on making it people centric.

We believe that the initial idea with which the App was conceived, of fighting an uphill battle with technology holds merit, and we propose the following changes that strengthen the rights framework without compromising on any functionality of the App.

2. Privacy Central to Mass Deployment of the App

For contact tracing to be successful, it must be deployed at a mass scale where citizen's trust of the App will be central to its usage. Trust cannot be built without transparency and accountability from the Government as a social contract between the citizen and the state.

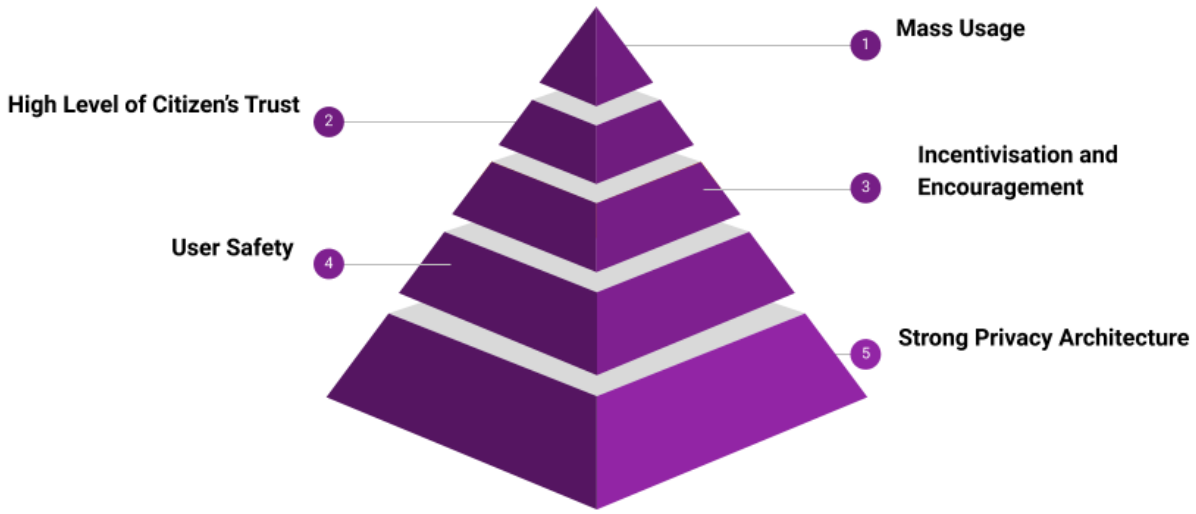


Figure 3.0

2.1 Citizen Trust is Critical

Figure 3.0 represents the relationship between various facets that are involved with respect to building the citizen's trust towards the App's deployment. A strong privacy architecture lies at the base of the pyramid, which the authors believe is vital for the successful mass deployment of the App. As per Figure 3.0, we believe that a trust-based system is more effective. This can bring people to exercise their discretion to voluntarily download the Aarogya Setu App, and they may be more comfortable, in general, to download it when not mandated to do so. The foundation of

building people's trust lies in encouraging them and building awareness on the need to download the App, which is also accompanied by promising user safety to them. This promise cannot be delivered without having a robust privacy architecture and framework as proposed in Section 3 of the paper.

Instead of forcing people, the Government should encourage and incentivise professionals working in public and private spaces to deploy the App. Mandated or forced downloading of the App faces multiple implementation challenges. Firstly, access to smartphones or internet connectivity is limited and may not be affordable for everyone. And secondly, the imposition order is unclear on whether the professionals have to use the App only while they are reporting to work, as employers might not be in a position to request their staff to use the App during non-working hours. Moreover, keeping track of all private professionals to download the App is beyond state capacity and might attract judicial overview in the future.

As we are facing an exceptional circumstance, the people of India may be willing to place their benefit of the doubt on the Government, and will trust them to do the right thing by ensuring that all checks and balances are adhered to and no harm is caused while at the same time protecting their privacy. The Government must repay this trust by placing all measures in place to prevent violation of their right to privacy and preventing future harm.

2.2 Immediate Solution Vs. Preventing Future Harm

The Government is pushed against making two choices in real time - whether to maximise technology input in the shortest span of time thereby limiting the spread of the virus; or deploying strong checks and balances to prevent future surveillance. We believe that there needn't be a choice between the two options, although it is imperative to ensure a high-level of compliance in both the choices at present.

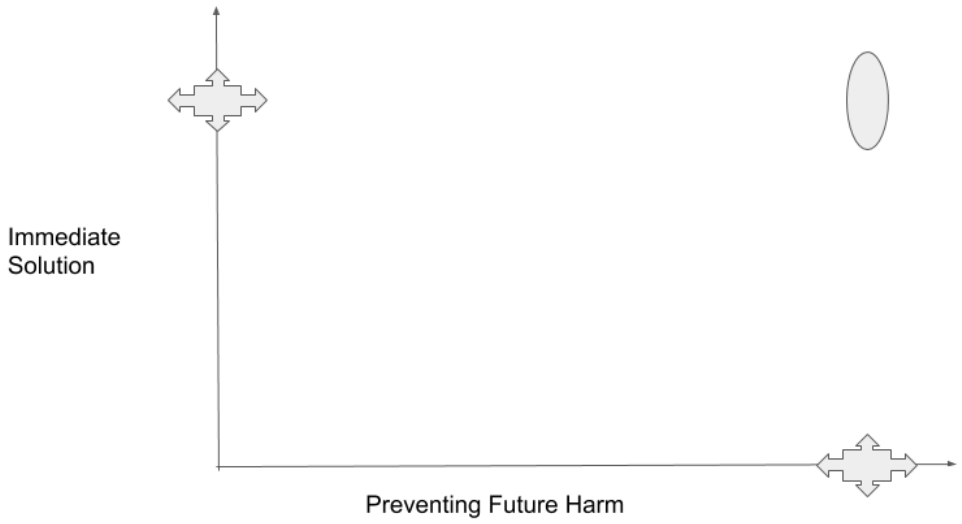


Figure 4.0

For the Government to derive an immediate solution that relies on aggressive use and deployment of the App, mass usage is fundamental. In Figure 3.0 we demonstrated that without a strong privacy architecture, it is difficult to enable user trust to drive mass use. Therefore, it implies that privacy is not only critical to ensure that long term harm is prevented by creating enough checks and balances to prevent surveillance, but privacy is also fundamental to activate the use of the App, as without consumer trust and incentivisation for mass use, contact tracing cannot be successful. The ideal scenario for the Government is to deliver on the symbol plotted on the graph in Figure 4.0,

where we maximise the immediate impact to curb the spread of the virus, while ensuring that its done in a manner that is completely safe and protects privacy of the people. The choice must not be between the two, but must include both. To invoke Gautam Buddha, we must strive to arrive at the 'middle path'.

2.3 Community Rights Vs. Individual Rights

The Government is facing another dilemma - ensuring that the individual's right to privacy is maintained while at the same time communities across the country do not fall victim to the chain of the virus. In times of a public health emergency of such gigantic proportions, the individual cannot be isolated from the community. The responsibility of the individual towards their community is greater than in a 'business as usual' scenario. As the virus spreads at a rapid pace once the host comes close in contact with their neighbour, the individual has a moral obligation on those around them to take maximum precautions and preventive measures in place.

Historical authority for quarantine stems from the idea that a public health contract exists, under which individuals agree to forgo certain rights and liberties, if necessary, to prevent a significant risk to other persons.[11] This contract is not only between an individual citizen and the Government, but also among citizens with each other. The Supreme Court of California In re Culver[12] confirmed the right of the Government to pass quarantine laws and envisage individual duties to protect the nation during an emergency. Also during the SARS outbreak in 2003, the WHO acknowledged that combining quarantines with surveillance and travel restrictions sharply reduced the adverse effects of the outbreaks and was necessary.[13] Therefore, while it is important that the privacy of the individual is protected, it is equally important that individuals practice the art of social distancing and responsible behaviour by abiding with norms to prevent getting in contact with a host.

[11] Barbera, J., et al., Large-Scale Quarantine Following Biological Terrorism in the United States: Scientific Examination, Logistic and Legal Limits, and Possible Consequences, 286 JAMA 2711, 2712 (2005).
[12] In re Culver, 187 Cal. 437, 202 P. 661 (1921), (California Supreme Court).
[13] World Health Organization, First Global Consultation on SARS Epidemiology, Travel Recommendations for Hebei Province (China), Situation in Singapore-Update 58 (May 17, 2003), Retrieved from: http://www.who.int/csr/sars/archive/ 2003_05 17/en/print.html.

At the same time, it is also important to note that the privacy of the infected and high risk individuals is protected to prevent social stigmatisation once they re-enter the community. Moreover, leaking the information and sensitive healthcare records of patients, infected people or recovered people might expose them to their physical community, which could be potentially harmful. Therefore, privacy is not just important from an individual's rights perspective, but also from a community rights perspective, and therefore an important aspect to the Right to health. As depicted in Figure 5.0, the Government should seek to maximise individual rights by according the highest levels of privacy, while at the same time ensuring that community is protected as a whole as well.

The ideal decision for the Government would be as plotted below in Figure 5.0, where once again, the Government is not forced to choose between an individual's or community's rights, but protect both by affording them the highest level of safety.

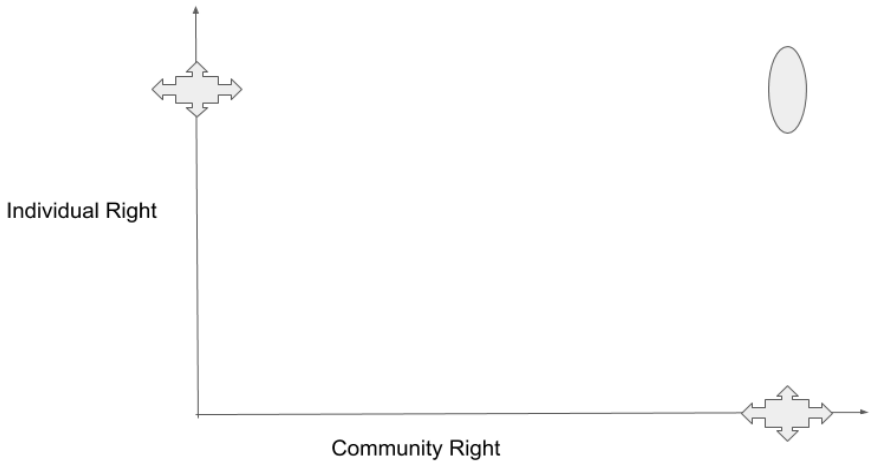


Figure 5.0

3. The Privacy Framework

3.1 Legality

Concern: Aarogya Setu, though well intentioned, falls short of widespread public confidence. It's mandatory use has raised questions of restricting the *right to privacy,* **without a law that is specific and explicit with respect to the rights that it seeks to infringe and the procedural safeguards that it establishes**. Further, various states have published details like the name, home address, travel history etc. of infected patients or those under quarantine. Health data should be confidential, and any such leak not only violates privacy and individual autonomy, it also degrades public trust among the people.

Solution: The Prime Minister's Cabinet must consider advising the President to pass an Ordinance[14], as the Parliament is not in session and cannot be called in times of such public health emergency. An Ordinance can not only legitimise the executive mandate to 'download' the App based on certain predefined considerations but can also establish procedural safeguards which would inspire public confidence. Also, no post pandemic laws requiring compliance have any applicability on this App. As stated by Justice Chandrachud in the Puttaswamy judgment, *"If the state preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it".*

Reason: The *Puttaswamy* judgement mandates that right to privacy may only be curtailed per a law which has a legitimate purpose. Any law restricting fundamental rights needs to spell out the right which it seeks to infringe, the basis of the infringement, and the procedural safeguards that it establishes, amongst other things. An Ordinance would suffice the need of such law which may be passed by the Parliament once it reconvenes. Standing on the anvil of transparency and accountability, the Ordinance would be an important milestone to garner public trust. In the words

[14] Article 123, Constitution of India.

of Justice Kaul, *"[A]n invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable."*[15]

3.2 Transparency and Verifiability

Concern: There is no manifesto or website that details the project and the purposes thereof. **The Government has a prevailing policy on adopting open source code software.[16] However, this privilege has not been extended to the Aarogya Setu App.** As a result, the highest standard of transparency could not be achieved. Also, the technical specifications have also not been made public. The popular 'Trace Together' App details its technical specifications in a policy paper for the community to critically evaluate and understand.[17]

Solution: The Government should make the code completely open source including the android and iOS application along with the back end. Reproducible build techniques should be implemented to ensure that users can verify that the App is from an audited source code. Encouraging security research to reverse engineer the systems are important tests for robustness in which keeping transparency would help. Moreover, when the Government states that *"... in order to securely collect, store, transfer and process personal information, the Government is deploying encryption to secure data",* it should be transparent and clear which technique for encryption is deployed. The technique source code should be open sourced for better operation and effectiveness of the App. Lastly, the Government ought to clarify what constitutes 'medical' and 'administrative' purposes in the context of COVID-19.

Reason: As Justice Madan B. Lokur explained *"[T]he balance between transparency and confidentiality is very delicate and if some sensitive information about a particular person is made public, it can have a far-reaching impact on his/her reputation and dignity."*[18] Transparency is

[15] *Supra note. 9.*
[16] Policy on Adoption of Open Source Software for Government of India, Ministry of Communication & Information Technology, Department of Electronics & Information Technology, Retrieved from: https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf.
[17] Bluetrace, TraceTogether - An Overview (2020), Retrieved from: https://bluetrace.io/policy/.
[18] ABC v. The State (NCT of Delhi), 2015 SCC Online SC 609.

one of the core principles of securing privacy of individuals. The open source code will help in achieving transparency as well as improving security as the source code will be open to independent audit. Additionally, it will also help in generating public confidence in the App and in turn, confidence in the Government as well.

3.3 Voluntariness

Concern: For an epidemiologically significant efficacy, a contract tracing App requires a high degree of dissemination in society. This wide distribution must not be achieved by force, but only by implementing a trustworthy system that respects privacy and is voluntary in nature. **Originally, the installation of the App was voluntary however has now been made mandatory by the Ministry of Home Affairs vide order dated 1st May 2020.**[19] The revised guidelines make it mandatory for the public and private sector employees. The duty has been casted upon the head of the respective organisations to ensure that all employees download this App. Further, the guidelines make it mandatory for residents living in the containment zone to download the App. **Pre-installation of the App in smartphones to be sold in India has also been flagged as a concern.**[20] Earlier, the Ministry of Human Resources Development also circulated a letter to schools to urge students and their parents or family members to download the App. **Reportage regarding police taking legal action against citizens not having Aarogya Setu App downloaded on their smartphones has been most distressing.**[21]

Solution: The community should be encouraged to download the App on a voluntary basis. Only those working or living in containment zones where there is huge scope of contracting COVID-19 could be mandated to download the App, even though enforceability will be a challenge and therefore imposition of such orders might not yield the desired benefit the Government wants to derive.

[19] Ministry of Home Affairs (May, 1 2020) Order No. 40-3/2020- DM-I(A).
[20] Smartphones could soon come pre-installed with Aarogya Setu app: Report. The Indian Express. Published on 30 April 2020, Retrieved from: https://indianexpress.com/article/technology/tech-news-technology/aarogya-setu-installed-smartphones-by-default-soon-6386270/.
[21] Butani A., (2020), No Aarogya Setu App? Pay Rs 1000 Fine or face 6 Months Jail in NOIDA, Indian Express, Retrieved from: https://indianexpress.com/article/cities/delhi/aarogya-setu-app-fine-jail-noida-6394954/.

Such mandates must be enforced only after risk assessment in consultation with the District Administration is conducted, which is possible as the Government would be surveilling these areas physically as well. Additionally, the administration must consider raising awareness about the App by developing FAQs and video-clips to answer the probable question about privacy that may arise from the application, and perhaps explain the functionality and importance of the App over *'Mann ki Baat'*.

Reason: Voluntariness enhances the trust in the government. While discussing voluntariness Justice La Forest held that, *"the use of a person's body or space without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity."*[22] Moreover, it would be improbable to force people to switch the internet on to activate G.P.S. location or turn on bluetooth to exchange 'digital identities', as enforcing this is beyond state capacity. Therefore, voluntariness is the key to the success of the Aarogya Setu App for deployment at a mass scale. Measures creating awareness will help people participate with informed consent rather than fear of the virus. Positive rather than negative reinforcement not only inspires trust and confidence but also ensures compliance.

3.4 Data Minimisation

Concern: The privacy policy and the terms of use do not adhere to the principles of data minimisation and purpose limitation. Data sets, such as profession, have no relevance with contact tracing. There is no study or comparative analysis that explains why geo-location data collected at every 15 minutes or during self-assessment is relevant for contact tracing. **It is necessary that only those data sets are obtained that have a direct role to play in enabling contact tracing.** Additionally, though the privacy policy states that the use of data obtained from the application will only be as per clause 2 or to fulfil any legal requirement, the term 'legal requirement' has not been defined in the privacy policy. **The non-specificity of the term 'legal requirement' raises ambiguity in its use and has the potential of being misused.**

[22] The Queen v. Brandon Roy Dyment, 2 S.C.R. 417 (Canada Supreme Court).

Solution: The privacy policy ought to be amended to define the term 'legal requirement' that must be in consonance with the tests laid down in the Puttaswamy judgment. Necessity should be observed when data is being collected, while deciding between multiple options, retaining the data, etc., keeping in mind that the objective of the application is containment of the pandemic. For example, the use of both geo-location and bluetooth connectivity may be an overstretch. Lawfulness should be ensured by adhering and remaining within the realms of existing laws.

Any data point not necessary for contact tracing must not be collected. Further, there is a need to conduct a privacy impact assessment to ensure that the overall technology clearly establishes a case for collection and processing, safeguarding, storage and deletion of data. This assessment study, needless to state, should be made public and will form the edifice basis which an individual and even judiciary can assess the legality of impact on an individual's privacy. The privacy policy should clearly set out the purpose for which the data will be used. The use of this data apart from using anonymised data for statistics, research and academics should be strictly prohibited. The Government, in line with the Singaporean TraceTogether App, should consider explaining the importance of collecting each data set. This will inspire public confidence and trust in the App.

Reason: Purpose limitation and data minimisation are two key principles to ensure that maximum benefit arises out of minimum personal data collection. As in the 'Report of the Group of Experts on Privacy'[23] and also observed by Justice Chandrachud in the Puttaswamy judgement *"[P]ersonal data collected and processed by data controllers should be adequate and relevant to the purposes for which it is processed."* In the absence of a data protection law, these two principles will ensure that the fundamental right to privacy is curtailed only in circumstances that are required lawfully.

[23] Report of the Group of Experts on Privacy, Planning Commission of India, (16 October, 2012) Retrieved from: https://www.dsci.in/content/report-group-experts-privacyconstituted-planning-commission-india.

3.5 Anonymisation

Concern: Even though the privacy policy states that the data sets will be aggregated and anonymised, it does not mention the standards used for anonymisation. **Proper anonymisation techniques are critical to minimise risk for re-identification of these data sets. All data sets, including the initial identification data i.e., name, age, sex, profession, travel history and geo-location at time of App installation must be anonymised.** With regards to protection of naming of patients, as stated in Puttaswamy Judgement, *"An unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy".* This finds resonance in Regulation 2.2. of the Indian Medical Council Regulations which requires physicians to maintain patient confidentiality.[24] Medical records are treated as sensitive personal information within Information Technology (Reasonable security practises and procedures and sensitive personal data or information) Rules, 2011.

Solution: Anonymisation should be deployed to ensure a three-fold protection from: a) Singling Out - is it still possible to single out an individual, b) Linkability - is it still possible to link records relating to an individual, and c) Inference - can any personal or non-personal identifiable information be inferred concerning an individual?[25] The Government should allow independent auditors to regularly check the anonymised data sets. It should take note of different anonymisation techniques available and adopted around the world like randomisation, generalisation, differential privacy, noise addition, k-anonymity, l-diversity and t-closeness. A subject matter group should be formed from experts in the Indian Computer Emergency Response Team and National Informatics Centre or any other relevant nodal agency, to discuss the main strengths and weaknesses of each technique. It would help to design an adequate anonymisation process in this context. Also, the technology deployed to anonymise personal data must be announced publicly on the Government website, which is presently the technique called 'hashing' for data sets.

[24] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, Indian Medical Council, Retrieved from: https://www.mciindia.org/documents/rulesAndRegulations/Ethics%20Regulations-2002.pdf.
[25] Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, 0829/14/EN WP216, Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm.

Exception: Given the nature of cryptography, complete and irreversible anonymisation may be a challenge as both anonymisation and de-anonymisation techniques are advancing simultaneously.

Reason: Health data comes under the ambit of sensitive personal data. The *Puttaswamy* judgement (*privacy)* mandates that health data should be used only after it is anonymised. Using the best available technology for anonymisation is key to ensuring user privacy.

3.6 Storage of Data

Concerns: The initial identification data such as name, age, sex, profession etc, are stored on servers managed by the Government of India. As per the policy, these data sets will be retained as long as the account is in existence or 'for a period as required under any law'. Further, per clause 2(b) and 2(c) of the privacy policy, location data will be uploaded on the server in case the user is tested positive for coronavirus and has come in contact with any other person or if self-assessment is taken by the user.

This data will only get updated on the server in case the person is either confirmed with COVID-19, is symptomatic, or the self-assessment shows that the person is symptomatic. Per clause 3(b), this data will be stored on the mobile devices for 30 days. Moreover, the data will be stored on the server for 45 days in case of a person who has been tested negative for COVID-19 and 60 days in case of a person who is found positive.

The storage of initial identification data creates ambiguity with regard to the time frame for which data will be stored. Secondly, the 45 days and 60 days period is too long for the data to be retained on the server. Timelines should be based on medical relevance as well as the realistic duration for necessary administrative steps to be taken.

Solution: An alternate viewpoint states that only the mobile number and a permanent anonymised user ID should be stored in a centralised Government server. Information relating to proximity and duration should be stored on a user's phone, after which it is deleted on a rolling basis every 21 days. The particular ID should also be randomized and encrypted after every 2 weeks so that

tracing back becomes difficult. The private key to these temporary IDs could be held by a particular institution that has the sole authority to decrypt the information. It is important that a time frame be decided by the Government after which all personal identification data would be purged from the servers as well. Moreover, the data stored should be kept in the secured server which could be audited by independent experts.

Exception: Post the pandemic, only limited use of anonymised data for statistics, research and academics should be permitted.

Reason: Relying on the 'Report of the Group of Experts on Privacy' Justice Chandrachud observed in the Puttaswamy judgement, *"[A]fter personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures."*[26] It is important that the data stored be completely purged in due course of time in order to avoid any security risks as well as misuse of such data. Retaining these data sets makes it vulnerable to external interference and subsequent abuse.

3.7 Grievance Redressal Mechanism & Accountability

Concerns: The privacy policy gives the details of the grievance redressal office but shares **no guidance on how soon complaints will be addressed, or how users exercise their right to access and confirm. Also, concerns regarding the ease of accessing the grievance mechanisms, especially for citizens in rural areas need to be catered to. Lastly, the terms of use absolves the Government from any liability**, even if the App incorrectly finds someone to be symptomatic which leads them to being quarantined, the liability is critical as that allows the scope of a judicial review in the future.

Solution: In order to effectively cater to these necessary challenges the Government should:

[26] *Supra* note 9.*;* See also Report of the Group of Experts on Privacy. Planning Commission of India, (16 October, 2012), Retrieved from: https://www.dsci.in/content/report-group-experts-privacyconstituted-planning-commission-india.

Firstly, come up with an efficient and independent mechanism to ensure that any issues arising out of the applications are resolved within a limited time frame. *Secondly*, the aggrieved users should be provided with a copy of data processed about them and details of the sharing of their data. *Thirdly*, the Government should ensure that the grievance redressal mechanism is free of cost and should create hotlines for easy access, particularly for the benefit of citizens who may not be tech savvy and cannot use e-mails. *Lastly*, the scope of liability of the Government authorities, and their officials, must be expanded to include penal provisions for misuse or unauthorised use of the data for any purpose. Also, the terms of use must not rule-out scope for civil claims, in cases where harm is caused to the individuals. Needless to say, as a long-term measure, establishment of a Data Protection Authority vide a Data Protection Law is imperative.

Reason: In the absence of a Data Protection Authority, a duly constituted independent redressal mechanism will ensure accountability for any misuse of the data. It will also help in enhancing public trust. An individual will have the right a) to know/obtain any data pertaining to it, b) receive communication in an intelligible form so that they can redress grievances, if any, c) to challenge any claim, if rejected, d) to have the data erased, rectified, completed or amended if the claim is successful.

3.8 Sunset Clause

Concern: The privacy policy and terms of use of the **App do not specify when the anonymised data sets stored in Government servers are to be purged completely after the pandemic ends. The legal framework should outline the duration of the restrictions in place and their geographical reach.** Blanket and indiscriminate collection and retention of data creates risks of abuse of civil liberties and civil rights.

Solution: The privacy policy and terms of use must clearly mention that the App and the anonymised data sets collected will be deleted entirely post the COVID-19 outbreak. The systems should be designed in a manner where it automatically stops processing of data and meta-data, and deletes both of it. The legal order should subsist only till the circumstances warrant it. An inspiration can be drawn from a number of sunset clauses introduced in the USA Patriot Act framed

in the aftermath of September 11th attacks, in which 16 sections of this legislation were originally meant to sunset on December 31st, 2005.

Exception: Only limited anonymised data to tackle future pandemics in India may be stored after ensuring that the same is ***not attributable*** back to individuals or communities that may be used to their disadvantage by an independent auditor. Further, such data should not be used for any other purposes, such as law enforcement. A list of which bodies/departments/institutions would be able to access retained data post-COVID should be made transparent.

Reason: Principles of privacy envisaged in the Puttaswamy judgement mandate that the right to privacy must be restricted to the period 'necessary', thus the personal data collected must be deleted once the pandemic ends to prevent risk of mass surveillance and function creep, amongst others.

3.9 Access to Data

Concern: The privacy policy and terms of service of the App are silent on the mechanisms deployed by the Government towards the collection of personal and anonymised data sets, which is fundamentally opposed to the idea of fair data processing. **Location data can be very revealing and intrusive in nature. Without proper caveats, access to such data might deduce even more sensitive information, such as religion, caste, address details etc. Additionally, the privacy policy does not mention which exact Government department will have access to the data collected via the App.**

Solution: The privacy policy and terms of service must clearly mention which department, such as, - the Ministry of Health - will have access to the data collected. The access to data must only be given once it is structured in an aggregated or anonymised form. For example, we can learn from Belgium and Germany where the data collected by the App is given partial access. A legal framework should be framed in which datasets could be shared with third parties only for a specified purpose and at particular times. Thus, the usage of vague phrases like *"necessary medical and/or administrative purposes"* should be avoided. Moreover, all the necessary

authorities/departments that would be given access to such critical data sets must be made public under the R.T.I. Act.

Exception: While the list of officials with the right to access may be simply updated on the Government website, any addition or change in the departments that may be given access to the critical data sets should require explicit consent of the users.

Reason: Access to data should be given with consent or via a lawful contract. Either way, the user should be informed of who has authority to access, process and with whom the data is shared. Justice Chandrachud relied on 'Stanford Encyclopaedia of Philosophy' and held *"[B]ehavioural privacy postulates that even when access is granted to others, the individual is entitled to control the extent of access and preserve to herself a measure of freedom from unwanted intrusion".*[27] Without such rights being clearly spelt out, fairness is compromised and so is the legality. Further, this creates an apprehension that the data can be accessed by any Government official and department, for any purpose. This feeds into the fear of mass surveillance.

3.10 Data Sharing

Concern: In a public health emergency, information such as location history, symptom reports, demographic information, or similar should be shared with public health officials or researchers under a proper legal framework. The privacy policy explains that the data collected will not be shared with any 'third party' but may be shared with 'healthcare providers'. **This begs the question: what will be the protocol for sharing the data with healthcare providers?**

Solution: A detailed protocol for sharing of such critical data with healthcare providers and where relevant protocol for 'processing' of such data by the latter must be drafted. Users should remain in full control of their personal data and it should be shared only with their consent. In such circumstances, legal data requests require transparency of what type of information is being asked

[27] Stanford Encyclopaedia of Philosophy (2002), Privacy, Retrieved From: https://plato.stanford.edu/entries/privacy/ See also: Cohen,J, "What Privacy Is For", Harvard Law Review (2013), Vol. 126, at page 1904

for (meta data or real-time insights), and what access has been granted. An example can be taken of 'Trace Together' where once a person is declared as infected, a temporary ID is shared with those devices which were nearby. This temporary ID is updated by the application periodically, rendering the identification of the infected impossible. Further, the data should not be shared, strictly, for any non-health purposes. The protocol must also enshrine the penalties for any violation of the protocol by the healthcare provider.

Reason: The list of healthcare providers who will need access to such data will be humongous and will include frontline workers, insurance companies and volunteers among others. It is imperative that they be briefed appropriately about the critical nature of the task that they are carrying out and the impact of any leakage of such critical data.

3.11 Integration of Data Sets

Concern: Both privacy policy and terms of service are silent on **whether the Government can compile or integrate the data collected via the App with existing health care data collected in India by the Government, autonomous or private entities.** The Integration of databases will not sustain the proportionality test laid down in *Puttaswamy judgment*.

Solution: The privacy policy must be amended to mention that the data collected via the App will not be integrated with existing health care data collected in India by the Government, autonomous or private entities. This would require building in the Fair and Information Practice Informational Principles into the Terms of Service and Privacy Policy.

Reason: If the data collected via the App is compiled or integrated with the health data collected by the Government, autonomous or private institutions then it will be very difficult to delete such integrated datasets as well as the inferences drawn thereof at a later stage. Without a sunset clause, integration of databases is a heightened issue.

3.12 Scope/Function Creep

Concern: The App may be utilised for purposes other than contact tracing, identification of hot-spots etc. **Some of the other purposes are mentioned in its terms of use - to include additional services which go beyond the primary purpose of the App like issuance of 'e-passes'.**

Solution: The App and any data collected must be used exclusively to combat COVID-19 infection chains. Any other use must be technically prevented as far as possible and legally prohibited to prevent data aggregation and thereby surveillant assemblage. The features which are not necessary to the principle objective of the App must be avoided. At the very least, the App must only be one way of attaining, say, an e-pass and preferably other equally accessible option(s) of attaining e-passes must be available to the citizens.

Reason: Issuance of e-passes requires access to 'government authorised I.D. Cards'. This adds to the data submitted via the App and should only be deployed per the principle of Data Minimisation.

3.13 Auditing

Concern: The hallmark of a true democracy is transparency and accountability. Accordingly, the **adherence of protocols for collection, processing, sharing, and accessing the data during the pandemic and deletion of the data post the pandemic must be ensured.**

Solution: An independent auditor who is either subject to Parliamentary or Judicial oversight must audit whether protocols for collection, processing, sharing, and accessing the data during the pandemic and deletion of the data post the pandemic were complied with. The audit ought to be conducted on a quarterly basis at both central and state level. The contact tracing Apps should be open source: - only the source code - and not the entire application, so that it is secure from intervention by malicious actors. Moreover, the independent auditor should do an in-depth formal analysis of the protocol and the report should be published subsequently. The complete source code for the App and infrastructure must be freely available without access restrictions to allow audits by the auditor.

Reason: The State has the right to restrict privacy for necessary state functions and to respond to public health emergencies. But this end ought to be achieved while respecting the fundamental principles of 'necessity' and 'proportionality' and the State too must be held accountable if the restrictions are not reasonable.

3.14 Public Confidence

Concern: For effective contact tracing, engendering trust is paramount. **The individuals may not be aware of how and when their privacy is being restricted**. The Government and the developers should be sensitive towards the rights and interests of people who will be impacted by the deployment of contact-tracing technologies. Success of any technology depends upon the massive voluntary adoption of it, which, without trust will lead to its failure. Involuntary adoption, violates rule of law and constitutional imperatives. The example of Iran must be considered, where citizens were concerned that a contact-tracing App was deployed as a spyware and collected insights on millions of Iranians.[28] This defeated the public trust as the App was in violation of the purpose limitation principle.

Solution: The privacy policy, terms and the technology used by the App must be explained in simple terms and perhaps with pictorial description for the common man to understand. Inspiration may be drawn by the description of the functionality and privacy measures of 'Contact Tracing App' being co-developed by Apple and Google.

Reason: The citizens have a Constitutionally guaranteed 'Right to Know'[29] and 'Right to Reasonable expectation of Informational Privacy'[30] which must always be respected by the State.

---

[28] Vice News (2020), Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People. Retrieved from: https://www.vice.com/en_us/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people

[29] R.P. Ltd. v. Indian Express Newspaper. 1988 SCR Supl. (3) 212.

[30] Katz v. United States. 389 U.S. 347 (1967)