J. Indian Inst. Sci.
A Multidisciplinary Reviews Journal
ISSN: 0970-4140 Coden-JIISAD

REVIEW ARTICLE

The Privacy Implications of Using Data Technologies in a Pandemic

*Rahul Matthan**

Abstract | The COVID -19 pandemic has seen a rise in the deployment of digital health technologies. This includes those aimed at identifying the infected and making sure they did not spread the infection any further as well as other technologies providing data driven insights aimed at improving the effectiveness of decisions such as locking down certain areas and allowing others to re-open. This paper attempts to evaluate the socio-legal implications of the use of these technologies with a particular focus on privacy. It does that by examining a range of data technologies that were deployed during the pandemic with a view to assess the socio-legal implications of their use. It analyses the technologies themselves, the data collected, the manner in which it was intended to be used and the safeguards if any built into these technologies. Based on this analysis we will attempt to evaluate the privacy implications of these technologies. Never before have data technologies been used in this manner at the frontlines of our battle against a virulent disease. As a result there are no precedents that directly address what does or does not constitute a violation of personal privacy. Notwithstanding that, the paper attempts to arrive at a conclusion as to the legitimacy of the use of these technologies and the safeguards that would be appropriate under the circumstances.

1 Introduction

The novel coronavirus (COVID-19) pandemic has given rise to a renewed interest in the digital health data. The urgent need to quickly curb the spread of the disease encouraged the development of a number of technologies[1] aimed at identifying those who were infected and making sure they did not spread the infection any further. Some of these technologies were distributed in the form of mobile apps that citizens were exhorted to download and use at all times. Others were deployed by fiat by state governments and local municipal and law enforcement agencies in an attempt to enforce quarantine and isolation orders.

In addition, there was an entirely different class of technologies that focused on generating useful data driven insights from easily accessible aggregate datasets. These technologies used the vast oceans of personal information managed by telecom and social media companies to build mobility models of urban areas to provide insights as to appropriate steps that need to be taken to most effectively manage the disease.

The use of data in this manner to map epidemiological spread was pioneered during the cholera outbreak in Haiti[2] and has since been used in the ebola outbreak in Sierra Leone[3] and the dengue outbreak in Pakistan[4]. In all these cases, by plotting call data records against map information it was possible to show how people move within defined geographical areas. In the context of cholera and ebola, this sort of granular mobility data allowed the respective governments to determine the urban areas that would most likely be hit next by the outbreak giving them valuable advance information to take steps to halt the spread of the disease.

[1] Bangalore, India.
*rahul@rahulmatthan.com

Each of these technologies raise a variety of socio-legal concerns[5]. Some technologies tracked and monitored the movement of individuals infringing upon their privacy and their right to be left alone[6]. Others analysed personal data to try and establish those who were likely to have been infected and in the process spied upon countless others who were as yet uninfected. The utilisation of data and digital technologies in this manner raises all sorts of questions with regard to the legitimacy of these measures as well as the proportionality of data actually collected[7]. Depending on how long the data that was collected was retained and the purposes for which it was used, various ancillary privacy concerns arose.

To the extent that these technologies were being operated and managed by private entities or, for administrative and medical reasons eventually transferred to private persons, there were concerns that allowing private companies access to this data posed an unacceptable risk to personal privacy. Where these technologies were being managed and operated by the state, the extent to which their use was being coerced raised questions as to the legitimacy of the actions of the State—even in these exceptional times. Given the type of information being collected, the stated purpose and the ultimate use it was being put to, questions were raised as to the proportionality of data collection.

The primary issue is one of personal privacy. By their very nature, all these technologies collected deeply personal data that no-one (private company or government entity) would have had any justification collecting had it not been for the extreme situation we found ourselves in. India does not, at the time of writing, have a data protection law. The draft Personal Data Protection Bill, 2019[8] is still pending with the Joint Parliamentary Committee[9] and under the circumstances it is likely to be a long time before it is presented before the Parliament. In the absence of a law there are no meaningful restrictions on the data that can be collected, the purposes for which it can be used, the duration for which it can legitimately be stored and the manner in which those from whom the data has been collected can get redress for their grievances.

If these technologies are being operated by the government (whether at the state or the central level), to the extent that they could violate the personal privacy of citizens, they would need to abide by the requirements of the three-fold test set out in the decision of the Supreme Court in *Puttuswamy v. Union of India*[10]. This means that no such technology can be mandatorily imposed on a citizen without the backing of a law. The State must demonstrate the existence of an over-arching State need that such justifies such a violation of privacy and having done that must demonstrate that the data that has been collected is proportionate to such need[11].

While the Government of India has, in numerous different contexts, invoked the Disaster Management Act, 2005 to support the many actions it has taken in the context of the COVID-19 epidemic[12], there are different views as to whether the legality limb of the three-fold test under Puttuswamy can be satisfied by issuing a notification under an existing law. On the one hand, it has been suggested that the reason why the Supreme Court imposed the legality requirement was to ensure that if the Government was going to impinge upon the privacy of its citizens it should only do so after going through the legislative process. It would completely subvert this fundamental safeguard if all it took to impose such a technology was an executive notification[13]. On the other hand it is impossible to ignore the unprecedented times that we find ourselves in. The purpose of enacting a legislation like the Disaster Management Act, 2005 was to strengthen the hand of the government in times of extreme emergency. It has, therefore, been suggested that to use all means appropriate in times of emergency would not be out of line.

There is little doubt that there is an over-arching State to take all steps necessary to manage the epidemic. However, the question in the context of each of the technologies mentioned above is whether or not the methods used by the State to achieve these ends are proportionate.

This paper examines the various data technologies that have been deployed during the pandemic with a view to assess the socio-legal harms that could result from their use. It will first discuss the various technologies that have been used in an attempt to understand the data collected, the manner in which it was intended to be used and the privacy safeguards if any built in to these technologies. Based on this analysis we will attempt to evaluate the privacy implications of these technologies. This is the first time that data technologies have been used as one of the lines of defence to contain the spread of a virulent disease. As a result there are no precedents that directly address what does or does not constitute a violation of personal privacy. Notwithstanding that, the paper attempts to arrive at a conclusion as to the legitimacy of the use of these technologies and the safeguards that would be appropriate under the circumstances.

The three-fold test to evaluate whether the actions of the State violate the right to privacy of the citizen are:
1.Does the State action have the backing of law
2. Is there an over-arching State need that justifies this violation of privacy.
3. Is the data collected proportionate to the stated need.

2 The Use Technology in the Pandemic

A number of different technologies were designed to help combat the COVID-19 pandemic. By far the largest variety of technologies were designed and deployed to target the individual. Since infected people may not show any visible symptoms and yet be contagious contact tracing had to play an important part in combating the epidemic. In addition, it was important to ensure that everyone who tests positive was kept away from those who were still uninfected—even if they were not suffering any debilitating symptoms.

These technology solutions were developed to augment the administrative and regulatory measures that were deployed by the State to curb the spread of the disease. In this section I will discuss the key technologies that were developed to combat the virus.

2.1 Contact Tracing

Contact tracing technologies are designed to collect the data of everyone a person comes in contact with so that when they tests positive for COVID-19 everyone they had come into contact with over the past few days in the past can be identified. This allows those who might have been infected when the transmitter of the disease was still asymptomatic and who might themselves still be asymptomatic to get priority tested so as to allow them to self-isolate as soon as possible rather than continue to spread the disease.

The Government of India developed an app called *Aarogya Setu*[14] whose stated purpose was contact tracing. Similar apps were developed by State Governments and various private entities. The Indian Institute of Science developed the *GoCoronaGo* app[15] for use within its campus and various corporate entities developed similar applications that were offered to employees as part of the official suite of corporate apps.

All these apps leveraged bluetooth services on mobile phones to record the details of persons who came in close proximity with each other in order, thereby building a database of contacts that was subsequently be accessed to notify them of their risk of having contracted the disease. When a phone on which the app is installed comes in close proximity with another such phone, the apps on both devices swap certain information specific to the contact (the unique identity of the user and the duration and proximity of the contact). This information is stored securely on both devices and is not accessible to either user. If any one of these users test positive for COVID-19 all the persons with whom he/she came in contact over the past few days are informed.

The Government of India's app, Aarogya Setu, was designed to operate in a quasi de-centralised manner. Information was designed to remain on the device by default and was only pulled from the app and uploaded to a secure server managed and operated by the Government of India in the event the user tests positive for COVID-19. All the contact information extracted from the phone in this manner is analysed to evaluate those that actually have a risk of being infected. It is only these persons who are notified or contacted so that they can receive appropriate medical attention[16].

Aarogya Setu: stores the information it collect on the phone by default. This information is encrypted so that even the user cannot identify the persons they have come in contact with. Information that is not pulled to the server is deleted from the phone every 30 days on a 30 day rolling cycle.

All contact information that remained on the device was stored securely in the App, in such a manner that even the registered user of the App could not identify the personal details of the users he or she came in contact with thereby protecting the privacy of the contacts. This information was deleted every 30 days on a 30 day rolling cycle thereby ensuring that data was not retained for longer than was required to serve the purpose of identifying the individuals contacted.

The Aarogya Setu app collects two types of data—demographic information (name, mobile number, age, sex, profession, countries visited in the last 30 days and smoking history) collected at the time of registration; and user information (personal information and location data) collected from the devices of other registered users with which the app came in close contact.

It was only when a person tested positive for COVID-19 based on a virological test that is reconfirmed by the ICMR, that the contact information stored in that person's App was pulled to a government server, where it was analysed for the purpose of identifying who among the list of contacts on the phone should be contacted and notified. The privacy policy of the App clearly states that data uploaded to the government sever would not be used for any purpose other than in relation to the management of COVID-19[17].

2.2 Monitoring Technologies

Anyone who has tested positive for COVID-19 should ideally be kept in isolation to avoid passing the virus on to those around them. This is particularly true of asymptomatic patients who are physically capable of moving about but would, if they did so, infect those they come in contact with. However, it has proven to be particularly[18] difficult[19] to keep infectious, yet otherwise healthy persons, isolated from those

around them during the pandemic[20]. Staying in isolation brought with it significant economic challenges[21] as well as social stigmatisation[22]. To enforce the isolation of infected and potentially infected persons, State Governments and local enforcement agencies designed and developed various technological solutions designed to leverage the location detection features that are built into modern mobile phones to inform law enforcement as to where the persons being monitored were from time to time.

The Tamil Nadu government launched a quarantine monitor that used mobile phone geolocation services to alert the police if the quarantined persons moved 500 m to 1 km away from the place, where they were supposed to be[23]. The Karnataka government made it a requirement for all those under quarantine to post, every hour, a selfie of themselves with their GPS coordinates embedded in the post[24]. The Maharashtra government created an app that combined both these features[25]. The Delhi[26] and Andhra Pradesh[27] governments eschewed the creation of an app simply using the mobile phone numbers of persons in quarantine to triangulate their location by requiring telecom companies to triangulate their location using cell towers data. Various other governments deployed drones[28] and facial recognition technologies[29] to identify persons who have violated quarantine orders.

2.3 Population Scale Mobility Tracking

COVID-19 spreads virulently through contact. What needed to be done, particularly in the early stages of the epidemic was to limit urban mobility in an attempt to slow the spread of the disease[30]. Modern technology is well placed to assist with this. Regulators with access to accurate data about urban mobility patterns would have been in a position to use this information to evaluate what measures that needed to be taken to optimally reduce movements of people in urban areas. The same data could then be reviewed to evaluate the impact of these regulatory measures so that further refinements can be evaluated and implemented[31].

Call data records (CDR) from mobile telecom companies were particularly suited to provide this information[32]. Since mobile penetration in urban areas is close to 100% in India, and since everyone keeps their mobile phone on their person all the time, every time these mobile phones ping nearby cell tower they leave a record of their location as they move through the city. The cumulative set of mobile tower pings describes the path that an individual makes in the course of the day. Individual CDRs, when aggregated and anonymised generate accurate population scale mobility patterns that can provide accurate information about the times in the day when mobility is at its highest and the locations, where the densest human-to-human contact takes place. Municipal authorities can use this data to determine what restrictions to impose and at what times in the day. After they have implemented travel restrictions they can once again study these mobility patterns to evaluate whether the regulations they imposed were successful or not.

A lesser known feature of the Government of India's Aarogya Setu app was the creation of heat maps – a feature that was subsequently called syndromic surveillance – by leveraging the self assessment feature of the app and co-relating that with location data to accurately identify emerging hotspots at a sub-post, office level well before health workers on the ground were able to identify them. Syndromic surveillance does not require personal data at all. It uses completely anonymised aggregate data to identify areas, where there is a high likelihood of an outbreak.

3 Socio-Legal Concerns

The primary concern with the use of all these technologies is the extent to which they infringe upon the personal privacy of citizens. Ever since the Supreme Court, in *Puttaswamy v. Union of India* held that there was such a thing as a fundamental right to privacy, all government actions that could have an impact on personal privacy are required to be tested against the three fold test set out in that decision. In other words, all such government actions need to demonstrate that they were (i) taken pursuant to a law, (ii) that the action taken by the government was justified to fulfil a specific State purpose and (iii) that the data collected is necessary to meet that purpose.

Of these three legs of the *Puttuswamy* test there is probably least amount of debate around the necessity leg. No-one disputes that it is the Government's duty to take all appropriate measures to safeguard the lives and health of its citizens in the face of this virulent and deadly disease. While we will only be able to assess exactly how effective these technologies actually were after the epidemic is over, it is unlikely that their deployment will be questioned on the basis of whether it was necessary to even try. That being the case, it is probably safe to say that all these technologies did serve a pressing State need. What remains to be seen is whether the other two legs of the

three-fold test—legality and proportionality—were met. If a given technology failed to meet any one of these tests it was liable to be struck down as violative of the fundamental rights of the citizens.

With that background let us proceed to examine the extent to which these technologies meet the legality and proportionality tests set out in the right to privacy judgment.

3.1 Legality

Given the suddenness with which the epidemic struck, governments had to mobilise themselves quickly. None of the technologies described above were deployed under the authority of a legislative enactment passed by parliament specifically authorising its use. As a result, in almost all circumstances, the technologies being used were deployed on the basis of executive orders or, even worse, based on the instructions issues by administrators who approved their use.

3.1.1 Contact Tracing

One of the primary concerns that were raised in connection with *Aarogya Setu* by its detractors was the lack of adequate legal backing for its use. There was no enabling law that was passed before the app was launched. While the government did issue a data sharing protocol[33] that set out the manner in which data collected by the app could be shared between departments of the government and research organisations, this protocol did not provide the sort of legislative support[34] that would have been necessary to deploy the app in the first place. All that the data sharing protocol did was regulate the manner in which data was shared by the departments of the government to whom it was given. This would not have been sufficient to defend a constitutional challenge against its legality.

Arguably, none of this is relevant, where the app is offered on an opt-in basis, where its use is voluntary. The question of the government violating the fundamental right to privacy of its citizens only arises when the citizen has no option but to use of the technology in question.

Use of Aarogya Setu was designed to be voluntary. It had a privacy policy that set out various privacy measures that had been implemented[35]. Users were required to agree to it as well as the terms of service when they first registered on the app. Users were free to refrain from using the app if they did not agree with the terms of the privacy policy, however, by registering themselves as users they were deemed to be bound by these terms.

That said, for a time during the initial lockdowns, the government briefly made the app mandatory[36] for all employees giving rise to concerns as to whether the consent provided under in terms of the privacy policy was in fact free[37]. The government eventually recalled its order making the app mandatory, converting this requirement into an exhortation to make best efforts to ensure widespread adoption. With that questions about the violation of the fundamental right to privacy on the grounds of legality were no longer relevant given that the use of the app was not being mandated. However, as the country opens up and the app starts to be made mandatory to travel on airlines and in public transport this question will need to be addressed from time to time in the context of the circumstances under which it is mandated[38].

3.1.2 Monitoring Technologies

With regard to the various monitoring technologies that have been discussed, there is no doubt that what they seek to do impinges on the personal privacy of the persons they seek to monitor. While these measures might be justified under the circumstances, their legality will depend on the law under which they have been deployed. To the extent that such data processing is voluntary, there is no need for legislative backing. However, wherever the use of the technology is mandated it will need a law.

Where apps are being used to monitor individuals in quarantine, one might argue that monitoring takes place with the user's consent. After all the apps through which this monitoring takes place have to be downloaded from the App Store and, before they are installed, the user has to accept their terms and conditions of use. In order for them to continue to be effective they must always be connected both to the mobile data network with location services turned on. All of these aspects are under the control of the user and by continuing to use these apps it could be argued that the user has consented to continue to make available the personal information that the app collects. Even in the absence of a specific privacy policy, persons who no longer wish to provide this information can simply uninstall the app, disconnect data and/or location services or simply leave their phone behind when they leave the quarantine location.

In actual practice, individuals being monitored by these apps are compelled to install them and keep them on at all times with location services switched on. If an app is not detected or in the event it does not send one of the messages it is required to send at the frequency that was mandated, local law enforcement agencies will show up and enforce compliance. Even though the app was voluntarily downloaded given this additional evidence of coercion it is quite clear that the constitutional requirement for legality was not met.

With respect to technologies that are based on compelling individuals to regularly produce evidence of their physical location—posting photographs of themselves or mandatorily keeping their phones on their person with location services active, user consent is irrelevant as collection is compelled. Similarly, where monitoring takes place by triangulating the location of the person's phone using cell tower information, no prior consent is obtained and the individual has no ability to withdraw from being monitored.

The Proportionality Test can be analysed in the context of the following privacy principles:

Purpose Limitation: the purpose to which the data will be put must be clearly notified. Use Limitation: once consent has been obtained for a stated purpose the data cannot be used for any other purpose.

Data Minimisation: only that much data can be collected as is necessary to achieve the stated purpose.

Storage limitation – data collected should be retained for no longer than is required to achieve the stated purpose.

3.1.3 Population Scale Mobility Tracking

Population scale mobility tracking relies on aggregated and anonymised datasets[1]. Most of these datasets are in the possession of private entities—social media and telecom companies. The underlying personal data from which these datasets were derived were collected in the course of the regular business activities of these companies with consent or, in the case of telecom companies, supported by legislation and the terms of the telecom license agreement with the government.

There is, at present, no restriction on the use by these companies of anonymised aggregate data sets so long as the underlying personal data from which they have been generated has been validly collected. While these datasets are created from the mobility information of hundreds of thousands of individuals, once anonymised sufficiently, the risk that any individual whose data is part of the mobility data set would be identified is minimal. The data being used to generate the results are, to that extent non-personal data that by its very nature poses no privacy risk. Accordingly, there would be no need to test these technologies against the legality leg of the right to privacy.

To the extent that Aarogya Setu uses aggregate anonymised data to generate heat maps of disease for syndromic surveillance, the fact that the information does not reveal any personal information about the individuals that make up the anonymised data set would suggest that there is no privacy violation that would require the backing of a law.

3.1.4 Proportionality

To be a proportionate exercise of state power, any action by the state must not be excessive when looked at in the context of the stated purpose for such action. When looked at in the context of data protection this principle laid down by the Supreme Court dovetails nicely with the privacy principles that are acknowledged around the world as being the cornerstones of data protection law – purpose and use limitation, data minimisation and storage limitation.

The principle of purpose limitation[2] stipulates that personal data should only be collected for a purpose that has been previously notified in clear and specific language. The ensures that data fiduciaries have to state their purpose for collection in clear and specific terms. They cannot, therefore, baldly request consent for all sorts of data collection as that would give them excessive access and the right to unhindered data collection. The use limitation principle states that data once collected for a purpose should not be used for any other purpose. This would include transfers for which prior consent has not been obtained.

The data minimisation principle[3] states that data fiduciaries should only collect as much data as is necessary to achieve the stated purpose. This is a further restriction on data collection in that it requires data fiduciaries to constantly evaluate whether the data that they are collecting (even if broadly permitted within the terms of the stated purpose) is actually necessary to fulfil the purpose.

The storage limitation principle[4] stipulates that data once collected should not be retained for longer than is necessary to fulfil the stated purpose. This applies as yet another fetter on data fiduciaries requiring them to continuously evaluate whether they still need to use the data

[1] One example of the use of mobility datasets in the fight against COViD-19 is the Covid-19 Mobility Network, a network of infectious disease epidemiologists at universities around the world working with technology companies to use aggregated mobility data to support the COVID-19 response. https://www.covid19mobility.org/

[2] Section 5 of the Personal Data Protection Bill, 2019 sets out the principle of purpose limitatio

[3] Section 6 of the Personal Data Protection Bill, 2019 sets out the principle of data minimisation.

[4] Section 9 of the Personal Data Protection Bill, 2019 sets out the principle of storage limitation.

that they had collected to achieve the stated purpose—and if the answer is no, to delete that data.

To evaluate whether these technologies meet the test of proportionality let's see how they stack up against these three privacy principles.

3.1.5 Contact Tracing

The *Aarogya Setu* privacy policy has a clearly stipulated purpose[5]—to use the contact data collected to identify people who have potentially been infected by COVID-19 and take appropriate measures to be able to combat the disease. The Data Sharing Protocol that was subsequently issued echoes that same purpose. It is impossible to test the use limitation principle (including any transfers that might have been made) without evidence or actual allegations of use or transfer contrary to the stated purpose. To the best of my knowledge, no such use or transfer has been alleged.

As far as the other data protection principles are concerned they have to a certain extent been implemented in the design of Aarogya Setu. The app collects a limited amount of information—demographic information that is used to stratify users along the lines that the disease actually stratifies the population and contact history which is the basic information that is required to make a contact tracing system work.[6] Contact information is deleted from the device after 30 days if it has not been used before that and from the cloud within a specified period of time.[7] Allegations have been made with regard to the fact that *Aarogya Setu* collects location information – data that is not required for contact tracing. While this is true location data is necessary in the context of syndromic surveillance and to that extent the collection of this information is necessary to achieve that purpose.

At least on the face of it, it would appear that *Aarogya Setu* adheres to the principles of purpose limitation, data minimisation and storage limitation. This would suggest that it meets the principle of proportionality set out in the Puttuswamy judgment.

3.1.6 Monitoring Technologies

App based monitoring services should be designed to collect only as much information as is required to achieve their purpose. In the case of apps designed to monitor people in quarantine should only collect as much information as is necessary to ensure that persons who need to remain in quarantine do so. The app should not access features of the phone that are not necessary to achieve this purpose (such as the microphone or other applications on the phone). The information collected by the app should be secured both in transit and at rest so that the information can neither be extracted from the phone nor while being uploaded to the cloud for analysis. Raw information (location as well as other data) should only be retained for as long as is necessary to establish that the person is in quarantine and should be deleted immediately thereafter. Information collected should not the used for any other purpose and should not be shared with any other agencies of the government or with private entities. If the only data that is collected is that which is required to establish that the person in question has remained in quarantine, then data collection would be proportionate. Any additional data collection would be a disproportionate violation of the right to privacy.

Since the purpose of these technologies is to ensure that persons who are supposed to be in quarantine remain there, the data collected must only be used to achieve that purpose. If it is used for any other purpose it would be disproportionate. If, for example, information of quarantined persons is published in any manner — whether on a public facing website or internally, where it can be accessed by multiple departments of the government, such publication would be disproportionate. In addition if the personal information collected is analysed for any purpose other than specifically establishing whether or not the person concerned remained within quarantine, such analysis would be disproportionate.

In relation to technologies that require selfies to be taken and regularly uploaded, the only information that should be collected is the photograph, the time it was taken and the GPS coordinates. If any other information is collected it would be disproportionate to the stated purpose. Once the photograph has been certified as matching the person in quarantine and the location details match the place, where he/she is being quarantined, its purpose has been served. There would be no need to continue to retain either the image or the location details any longer. Continued retention of anything more than the last picture uploaded would constitute a disproportionate violation of the privacy of the individual concerned.

[5] Ibid n.16 at Clause 2.

[6] Ibid n.16 at Clause 1.

[7] Ibid n.16 at Clause 3.

Where telecom data is being used to identify the location of individuals under quarantine, then the information collected should be limited to the time-stamped location information of the person in quarantine. If any additional information (such as calls made or other device information, etc.) is collected, such collection would be disproportionately excessive. The storage of continuous time-series data about the location of the individual concerned would be disproportionate to the purpose of ensuring that the person remains in quarantine. The only location data that should be retained is information pertaining to the breach of the quarantine restrictions and that too only until such breach has been rectified. Finally, the publication of the address and other personal details of persons under quarantine, would be a disproportionate violation of their right to privacy as there are many other less intrusive methods by which the state purpose of ensuring that they remain in quarantine can be achieved.

3.1.7 Population Scale Mobility Tracking

As discussed above, population scale mobility data is, by definition, aggregated and anonymised. This means that the data in question is not personal data, and therefore the question of using it proportionately does not arise.

That said, it is important that the entities using this data take appropriate care to maintain the anonymity of the data in all the actions they perform on it. Since the CDR datasets used in these models are an aggregation of the data points generated by each individual telecom subscriber, if not sufficiently aggregated, it would be possible to identify an individual's personal data from out of the aggregated data set. There is a particularly high risk of doing this when the number of distinct fields that comprise the data set is high and/or when the sample size of the data set is low. In a country like India, where population density varies significantly from urban areas to the rural hinterland, the cell size of a given population sample will need to be dynamically adjusted to achieve the appropriate level of anonymity.

Assuming a sufficiently high level of aggregation, it should be possible to achieve a great enough degree of anonymisation so as to make it is statistically unlikely that the individuals who have contributed their personal data to the aggregate dataset can ever be personally identified. If this were to be the case, the privacy risk of using these datasets would be significantly reduced. Given the over-arching state purpose to measure social distancing metrics, the use of this data under these circumstances would not violate the personal privacy of the individuals whose personal data has contributed to the aggregate dataset.

4 Conclusion

The urgency with which the disease descended upon us left the Government with few options and little time to react. While the medical machinery of the State swung into action, there was an unprecedented opportunity to use data to augment the efforts of health workers on the ground. Technology was deployed rapidly and across a wide range of use cases. In the hurry to build, test and rollout, in most instances, little heed was paid to the privacy implications of these technologies. Or the long-term social harms that they could cause. In most cases, once the dust settles and things get back to normal, the data collected and currently in the possession of various government departments across the length and breadth of the country will likely be challenged in court. When that happens it is the technology that adhered to the basic requirements of the three-fold test under the Puttuswamy judgment that will be upheld.

Any medical technology that collects data indiscriminately – either because no clear purpose was stated or because the data collected far exceeded the stated purpose – will have violated the proportionality requirement. Even where the purpose has been stated, to the extent that it has been phrased in broad, non-specific terms or where there is no justification for the wide sweep of purposes in the context of the State need sought to be achieved, there will have been a breach of the proportionality requirement.

Data once collected legitimately must the used only for the stated purpose and once that purpose has been met will have to be deleted. Medical technologies that fail to meet this requirement will have fallen short of what is required to meet the proportionality threshold. Data which is not deleted but instead retained and deployed for some secondary purpose would constitute a clear violation of the principles of privacy.

Finally, aggregated and anonymised data is generally considered to be outside the purview of both the right to privacy judgment as well as the privacy principles as commonly understood around the world and specifically reflected in the Personal Data Protection Bill, 2019. That said, all anonymised information is

capable of being re-identified. Furthermore, as more and more anonymised datasets are layered upon each other, so long as the information contained in them pertains to the same set of people, it becomes easier to infer identifying characteristics from out of these data sets. Care must be taken when dealing with these datasets to ensure that, either due to an ignorance of the implications of re-identification or as a result of sheer accidental oversight, the underlying personal information is not revealed.

As much as the use of data at this scale in a medical context is unprecedented, the opportunity to deploy technology in a way that support and supplements the efforts of the frontline health staff as well as the government healthcare machinery has been rewarding. Many of these technologies have demonstrated some success. However, it is only those that have managed to do so with minimal impact on personal privacy that will stand the public scrutiny that will inevitably follow.

Publisher's Note

Received: 12 August 2020 Accepted: 15 September 2020
Published online: 9 November 2020

References

1. Marr B (2020) Coronavirus: how artificial intelligence, data science and technology is used to fight the pandemic. Forbes, https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/. Accessed 12 Aug. 2020
2. Bengtsson L et al. (2015) Using mobile phone data to predict the spatial spread of cholera. Sci Rep 5(1):1–5. www.nature.com, https://doi.org/https://doi.org/10.1038/srep08923
3. Big Data for Development: Preventing the Spread of Epidemics. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/BigData/default.aspx. Accessed 12 Aug 2020
4. Telenor Research Deploys Big Data Against Dengue. Telenor Group, 8 Sept. 2015, https://www.telenor.com/media/press-release/telenor-research-deploys-big-data-against-dengue
5. Findlay M et al. (2020) Ethics, AI, Mass data and pandemic challenges: responsible data use and infrastructure application for surveillance and pre-emptive tracing post-crisis. SSRN Scholarly Paper, ID 3592283, Social Science Research Network, 4 May 2020. papers.ssrn.com, https://papers.ssrn.com/abstract=3592283
6. Palmer D (2020) Coronavirus Contact-Tracing Apps: What Are the Privacy Concerns? ZDNet. https://www.zdnet.com/article/coronavirus-contact-tracing-apps-what-are-the-privacy-concerns/. Accessed 12 Aug 2020
7. A Legal Framework for Digital Surveillance in the COVID-19 Pandemic - by Shashank Mohan and Divij Joshi. MediaNama, 14 July 2020, https://www.medianama.com/2020/07/223-law-contact-tracing-india-digital-surveillance-covid19-pandemic/
8. The Personal Data Protection Bill, 2020, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019. Accessed 12 Aug 2020
9. Personal Data Protection: Govt Refers PDP Bill To Joint Select Committee. Inc42 Media, 12 Dec. 2019, https://inc42.com/buzz/govt-refers-personal-data-protection-bill-to-joint-select-committee/
10. Puttaswamy V (2017) Union of India, Writ Petition (Civil) No. 494 of 2012, 10 SCC 1. https://indiankanoon.org/doc/91938676/
11. Bhandari V, Lahiri K (2020) The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World (April 20, 2020). 3(2) Univ. of Oxford Human Rights Hub Journal 15 (2020), Available at SSRN: https://ssrn.com/abstract=3580630
12. Covid-19: Disaster Act Invoked for the 1st Time in India. Hindustan Times, 25 Mar. 2020, https://www.hindustantimes.com/india-news/covid-19-disaster-act-invoked-for-the-1st-time-in-india/story-EN3YGrEuxhnl6EzqrlreWM.html
13. Bhatia G (2020) Coronavirus and the Constitution – XXI: The Mandatory Imposition of the Aarogya Setu App. Indian Constitutional Law and Philosophy, 2 May 2020, https://indconlawphil.wordpress.com/2020/05/02/coronavirus-and-the-constitution-xxi-the-mandatory-imposition-of-the-aarogya-setu-app/
14. Aarogya Setu. https://aarogyasetu.gov.in/. Accessed 12 Aug 2020
15. GoCoronaGo. https://gocoronago.app/. Accessed 12 Aug 2020
16. Aarogya Setu Privacy Policy. https://static.swaraksha.gov.in/privacy/. Accessed 12 Aug 2020
17. Matthan R (2020) Opinion|The Privacy Features That Are Built into Aarogya Setu. Livemint, 7 Apr. 2020, https://www.livemint.com/opinion/columns/the-privacy-features-that-are-built-into-aarogya-setu-11586279239882.html
18. Nolan P et al (2020) Man Offers People to Pay Rs 25,000 to Escape Quarantine in Bengaluru, Police Registers FIR. India Today. https://www.indiatoday.in/india/story/man-offers-people-to-pay-rs-25-000-to-escape-quarantine-in-bengaluru-police-registers-fir-1681263-2020-05-24. Accessed 12 Aug 2020
19. Booked and Arrested: 10 Coronavirus Suspects Who Escaped Home-Quarantine in Bengaluru Face 'Long Arm

of Law. DNA India, 30 Mar. 2020. https://www.dnaindia.com/india/report-booked-and-arrested-10-coronavirus-suspects-who-escaped-home-quarantine-in-bengaluru-face-long-arm-of-law-2819041

20. In Home Quarantine for Coronavirus? You Are Being Watched. The New Indian Express. https://www.newindianexpress.com/states/telangana/2020/mar/18/in-home-quarantine-for-coronavirus-you-are-being-watched-2118103.html. Accessed 12 Aug 2020
21. Rakshit D, Paul A (2020) Impact of COVID-19 on Sectors of Indian Economy and Business Survival Strategies (June 6, 2020). Available at SSRN: https://ssrn.com/abstract=3620727 or http://dx.doi.org/https://doi.org/10.2139/ssrn.3620727
22. Social Stigmatisation of Covid 19 Patients. Countercurrents, 9 Aug. 2020. https://countercurrents.org/2020/08/social-stigmatisation-of-covid-19-patients/
23. COVID-19: Tamil Nadu Police Launch App to Track Home Quarantined Persons. The Week. https://www.theweek.in/news/sci-tech/2020/03/26/covid-19-tamil-nadu-police-launch-app-to-track-home-quarantined-persons.html. Accessed 12 Aug 2020
24. Mar 31, TNN /. Updated: et al. Covid-19 in Karnataka: Quarantined? Upload Selfie Every Hour | Bengaluru News - Times of India. The Times of India. https://timesofindia.indiatimes.com/city/bengaluru/karnataka-quarantined-upload-selfie-every-hour/articleshow/74903644.cms. Accessed 12 Aug 2020
25. Maharashtra Government Launches 'MahaKavach' App to Help in Contact Tracing, Tracking of Quarantined COVID-19 Patients. Zee News, 1 Apr. 2020. https://zeenews.india.com/india/maharashtra-government-launches-mahakavach-app-to-help-in-contact-tracing-tracking-of-quarantined-covid-19-patients-2273218.html
26. Covid-19 Update: Inspired by Singapore, Delhi to Track Mobile Phones to Enforce Quarantine. Hindustan Times, 1 Apr. 2020. https://www.hindustantimes.com/india-news/covid-19-police-told-to-track-mobile-phones-of-people-under-quarantine-says-delhi-cm/story-2sZ90oirpjMrKbjnG1KNRI.html
27. COVID-19: Andhra Pradesh Uses Tracking Tools to Monitor Home Quarantine Persons, Trace Contacts. https://www.timesnownews.com/india/article/covid-19-andhra-pradesh-uses-tracking-tools-to-monitor-home-quarantine-persons-trace-contacts/571663. Accessed 12 Aug 2020
28. Tripathi R (2020) Covid-19 Lockdown: Authorities Rely on Drone Eye to Maintain Vigil. The Economic Times. The Economic Times. https://economictimes.indiatimes.com/news/politics-and-nation/covid-19-lockdown-authorities-rely-on-drone-eye-to-maintain-vigil/articleshow/75112745.cms. Accessed 12 Aug 2020
29. Pune Cops Develop Home Quarantine Monitoring App For Externed Criminals. NDTV.Com. https://www.ndtv.com/pune-news/coronavirus-pune-cops-develop-home-quarantine-monitoring-app-for-externed-criminals-2246242. Accessed 12 Aug 2020
30. Why Lockdowns Can Halt the Spread of COVID-19. World Economic Forum. https://www.weforum.org/agenda/2020/03/why-lockdowns-work-epidemics-coronavirus-covid19/. Accessed 12 Aug 2020
31. Oliver N et al (2020) Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. Sci Adv. https://doi.org/10.1126/sciadv.abc0764
32. Evans-Pughe C (2018) Mobile Maps: Mapping Live Data with the Help of Mobile Networks. 17 Apr. 2018. https://eandt.theiet.org/content/articles/2018/04/mobile-maps-mapping-live-data-with-the-help-of-mobile-networks/
33. Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 | Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/content/aarogya-setu-data-access-and-knowledge-sharing-protocol-2020. Accessed 12 Aug 2020
34. We Studied the Protocol: And No This Doesn't Sufficiently Protect Your Privacy. Internet Freedom Foundation, 13 May 2020. https://internetfreedom.in/we-studied-the-protocol-and-no-this-doesnt-sufficiently-protect-your-privacy/. Ibid n.16
35. India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy. MIT Technology Review, https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/. Accessed 12 Aug 2020
36. Ranjit T, Jain T (2020) An Exclusion Tale: Aarogya Setu's March From Optional to Mandatory. TheQuint, 6 May 2020. https://www.thequint.com/voices/opinion/aarogya-setu-app-from-voluntary-to-mandatory-and-mass-exclusion
37. Not All Air Travellers Need to Download Aarogya Setu App. Hindustan Times Tech, https://tech.hindustantimes.com/tech/news/not-all-air-travellers-need-to-download-aarogya-setu-app-71590313791280.html. Accessed 12 Aug 2020
38. One example of the use of mobility datasets in the fight against COViD-19 is the Covid-19 Mobility Network, a network of infectious disease epidemiologists at universities around the world working with technology companies to use aggregated mobility data to support the COVID-19 response. https://www.covid19mobility.org/

Rahul Matthan is a partner at Trilegal. He heads the Technology, Media and Telecommunications (TMT) practice group of the firm. Rahul has advised on some of the largest TMT transactions in the country. He has worked with companies across all sectors of the industry from big telecom operators, to new internet businesses and media operations. Rahul has also advised on a range of sectors in the technology space including in relation to data protection, outsourcing, electronic commerce, new media, entertainment, biotechnology, healthcare and other new technologies. He has advised on new content delivery models for mobile value added services, regulatory issues surrounding the delivery of electronic content and legal and contractual issues in global e-commerce. He has also been involved in a number of policy initiatives in the technology space including, assisting the government in preparing the country's privacy law. He is a published author and a regular speaker across the world on matter relating to emerging technologies and the law and he writes a weekly column on the interface of law and technology entitled Ex Machina in the Mint, a leading national business daily.Rahul now serves on the Board of Trilegal after having served for many years on the Firm's Management Committee.