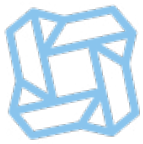

TANDEM
RESEARCH

# COVID-19 Tech Tools for Public Health

## Tandem Research | August 2020

This publication was first published by the authors under auspices of erstwhile Tandem Research.

# Contents

# 1. Why this Report?

As public health infrastructures globally struggle to cope with the Covid-19 pandemic, it is reasonable that governments are turning to technological tools to bolster their Covid-19 response. In India, as well, there has been a strong impetus for technology adoption in response to the pandemic.

However, in India, adoption has outpaced governance - with data-driven technologies continuing to operate largely in a legal and policy vacuum. For example, Aarogya Setu, the government's Covid-19 contact tracing app, has been criticized by civil society actors for violating privacy, possible misuse of data, and failing to adhere to existing legal frameworks.[1] However, Aarogya Setu is only one application amongst many being developed and deployed by state and private actors. Consequently, other applications have not received the same amount of public scrutiny and attention.

In May 2020, Tandem Research began tracking the adoption of technological tools to manage public health concerns related to Covid-19 in India. While in recent times, researchers and other civil society organisations have reviewed several of the applications and tools rolled out by respective state governments in India, our intention with the tracker has been to cast a wider net. This allows us to understand not just the forms of technological social contracts underway between states and citizens, but also the role of private technology companies. The broad goal of this report is to identify the challenges and gaps in provision of responsible digital health services in India during the pandemic.

It is indisputable that the pandemic requires a speedy and time-sensitive response. However, this led to the absence of public accountability and democratic deliberation in the rollout of many of these tools. The onus is thus placed on civil society to keep track of the technological trajectories embarked upon by both states and private actors in their hasty response to Covid-19. The need for responsible technological adoption is particularly critical to avoid undesirable technological and societal lock-ins. Quick fixes and rapidity of response cannot be framed as a tradeoff for ethical design and responsibility.

This report provides a review of the tools identified in our tracker, along selected parameters which include equity and inclusion; privacy and data protection; accountability and transparency; adequacy of current legal frameworks; scientific validity and efficacy; and potential for misuse.

These parameters, identified initially through secondary literature, were further revised through an iterative process, informed by the tools themselves, and the particularities of the Indian context. We view this report as a work in progress, and welcome feedback and suggestions.

The rapid review of tech tools for Covid-19 accompanying this report can be accessed at: www.techtoolsforCovid19.in

## Covid-19 Tech Tools for Public Health in India: in Numbers

- Currently, there are at least **85** different technological tools being used to augment the public health response to Covid-19 in India. These tools serve a wide range of purposes - from preliminary testing and screening, to location tracking and quarantine management.

- Of the 85 tools we have identified, at least **64** have been issued by the government of India, across different states and district administrations, and have been developed either in-house or in partnership with the private sector.

- There are **21** private sector backed tools, which are currently at different stages of development and deployment.

- Amongst the 64 government backed applications, **44** have been developed in partnership with private developers and tech companies, and only **32** have been developed in partnership with the IT departments and other government agencies.

- These tools rest on a number of different technological foundations. While some are backed by AI and IoT, others use GPS, bluetooth and cellular technology.

- Some tools also use robotics, data science and statistical analysis. Amongst that tools that are mobile-phone based, only **2** have accounted for feature phones and lack of digital literacy.

## 2. Responsible Tech in the time of Covid-19

While the literature on responsible technology innovation and adoption is diverse, a few common features and shared values underline what we understand by responsibility in the context of technology. These include values such as fairness, sustainability, human centered values (individual empowerment, social opportunity, and user safety), trust and transparency. Similarly, responsibility in technology has often been understood as that which is "(ethically) acceptable, sustainable, socially desirable, leading to socially desirable outcomes, care for the future, and taking account of social and ethical aspects and balancing economic, socio-cultural and environmental aspects."[2]

Schomberg (2011), for example, defines Responsible Technology Innovation as:

> "A transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)."[3]

Similarly, Stahl, Eden, and Jirotka, define it as:

> 'A social construct or ascription that defines entities and relationships between them in such a way that the outcomes of research and innovation processes lead to socially desirable outcomes.'[4]

Responsible technology then can be understood as a process or an approach whereby the outcome and processes of technological development and innovation are informed by broader societal values.

In India, the need for responsible technology becomes all the more important in light of the technologically driven response to the pandemic. Not only has the Covid-19 pandemic shed a sharp focus on the weak health infrastructure in India, but it has

also highlighted the inadequacy of existing legal and regulatory frameworks that govern technological development and adoption in India.

Further, government action during the pandemic is largely backed by dated legislative frameworks - the 1897 Epidemics Act and the 2005 Disaster Management Act[5] - which not only prove to be inadequate under current circumstances but also give wide exemptions to the state. The existing gaps within the two laws, has led to a situation of unilateral and ad hoc decision-making by different states in the country, as seen in the case of lockdown restrictions and their impact on migrant workers.[6] This further extends to the nature of technological adoption and deployment that is visible across different states.[7]

Several tech tools being adopted for Covid-19 in India, incorporate digital and AI technologies, which rely also on the capture of information and personal data of users. However, existing legislation such as the Information Technology Act, 2000 (IT Act, 2000), do not provide adequate data protection and security to individuals. While the recent Telemedicine Guidelines 2020 are a step forward in regulating emergent healthcare practices, much of the data protection framework for health data covered by DISHA guidelines has been dropped due to the PDP Bill (which is also yet to be enacted). Even if enacted, it does not protect an individual's health related data as strongly as the proposed DISHA guidelines would have.[8]

Even before the pandemic, there was much enthusiasm towards the use of technological tools to address the infrastructure and human resource gaps in the Indian health sector. While these tools signal a responsive state and the digital tech industry rising to the challenge of Covid-19, many of these tools are in fact a part of a larger health data industry that has been taking form in the past decade.[9] From the use of fit-bits to sleep tracking technology, health tech has permeated our everyday lives.

Further, because the pandemic constitutes a public health crisis, it refracts our understanding of responsibility in technological interventions along the trade-off between population health and individual freedom/rights.

However, how this dilemma is resolved in specific contexts is tied to a careful weighing of the associated harms and potential benefits. In the same vein,
the converse also stands true - in proposing a responsible tech innovation framework

in health (RIH), Silva et al suggest that in the domain of 'population health value', although innovation that provides individual health benefits is valuable, RIH should increase our ability to attend to collective needs whilst tackling health inequalities.[10]

Currently, the discourse around technological adoption for Covid-19 in India occupies a space of ambivalence between individual healthcare or population healthcare. On one hand, the rushed response to secure population health has resulted in intrusive measures of state surveillance and over-policing, with users being asked to forgo privacy for the good of public health. On the other hand, most tech tools in the form of mobile applications cater to a section of the population, who are consumers of digital health tech, with smartphones and internet connectivity. As a public health crisis, the pandemic also places immense pressure on fiscal resources and livelihood in addition to health infrastructure and in the context of Covid-19 in the Global South. These factors must be weighed in while developing our understanding of responsible tech adoption.

In such a scenario, we believe that we must widen the scope of what we understand by responsibility in the context of technological solutions to Covid-19. In the next section, the report presents a framework in development, which identifies six parameters, to assess and understand responsible tech adoption in the context Covid-19 in India. Each of these parameters have been further broken down into a set of guiding questions which seek to address responsibility in processes of both development and deployment, and are also firmly situated within the wider socio-political and legal context of India.

## 3. Method

The methodology consists of data collection of information related to various tools and apps that were developed/adapted in response to the pandemic. This was done through keyword searches on digital platforms (primarily, Google and Twitter) supplemented by a qualitative study (review) of a representative sample. The selected tools were reviewed against parameters outlined in this section.

## 3.1 Identification of Tools

To create an exhaustive tracker, the initial process of data collection was done through the use of extensive keyword searches such as ‘tech tools for Covid-19’ or ‘start-ups for Covid-19’ on Google, Twitter, and news sites, both national and regional. The scope of the search was narrowed to specifically the Indian context and only tools that included a software component.

The tools were then categorised into 6 groups on the basis of primary function and purpose:

1. Telemedicine
2. Remote Health Monitoring
3. Testing and Screening
4. Virus Mapping and Contact Tracing
5. Information and Alerts
6. Location Tracking and Quarantine Management

Further, the tools under each category were supported by identifying secondary functions, the developer, technology, and overall extent of adoption. This also assisted in the selection of a representative sample from each category. It must, however, be noted that the many of these tools so categorised perform overlapping functions. For example, many of the applications providing information and alerts also perform other functions such as contact tracing, or provision of telemedicine consultations. The categorisation of tools into different functions were therefore done on the basis of what the claims made by developers/deployers, where such information was publicly available.

The criteria for review was the extent of adoption or reach of the tools. Because of the dynamic and changeable context of the pandemic, news reports were relied upon to ascertain the extent of deployment (especially by the central or state governments). In the case of private sector tools, the number of downloads or deployment in medical colleges and hospitals was used as a proxy for adoption. The resulting sample involved 4-5 tools to be reviewed under each category.

## 3.2 Parameters for Evaluation

A study of pre-existing responsible technology frameworks, revealed several important approaches to reviewing the sample. However, since the tools under consideration were developed in response to the pandemic, it was important to develop a contextually rooted method of analysis. Based on a literature review of previous responsible technology studies, and the current context of the pandemic - 6 parameters were developed to review the tools:

1. **Equity and Inclusion:** Existing frameworks and literature on responsible tech adoption points to the need to assess the adoption and development of technologies from the perspective of the most vulnerable sections of society. In the case of Covid-19 tech tools, there is a need to assess the scale of adoption and accessibility amongst diverse socio-economic groups, including women, minority linguistic groups, people living in poverty, or otherwise digitally excluded.

2. **Privacy and Data Protection:** In the context of Covid-19 tech tools, particularly, in case of contact tracing apps, the infringement on individual privacy has become a huge concern. The recent Apple-Google contact tracing API, while contentious, however shows that technology need not compromise user privacy and tools can be designed to be privacy protecting design of technological tools. In the case of Covid-19 technological tools, there is a need to assess whether adequate measures to safeguard user privacy are in place.

3. **Accountability and Transparency:** The need for adequate measures of accountability and transparency is well recognised in the literature on responsible technology. In the context of Covid-19, this is particularly important, for two reasons. First, the presence of clear accountability and transparency measures help build public trust in institutions and technologies. This is particularly important since certain technologies, such as digital contact tracing, can only work if there is widespread adoption. Second, the need for accountability and transparency, in the form of rules regarding liability in case of harm, public channels of information dissemination and grievance redressal is even greater, with the invocation of emergency laws and slowing down of other channels of democratic opposition and accountability.

4. **Adequacy of legal frameworks:** As noted, several emerging and data driven technologies in India continue to be outside the purview of strong legal frameworks. However, certain provisions under the IT Act, 2000, as well the new Telemedicine Guidelines, do provide some legal and regulatory guidance (discussed in detail in the following sections). Two questions become important here. One, whether the operation of these tools adhere to the provisions of existing laws, and regulations and more importantly, whether existing laws provide adequate legal protections to citizens.

5. **Misuse:** The concentration of power, as well as the absence of strong legal protections for citizens in the context of digital and AI based technologies, has given rise to concerns regarding the misuse of technologies, including but not limited to, surveillance, function creep as well as data theft. In assessing tech tools for Covid-19, the potential of misuse leading to wider societal harms must be analysed. This is particularly significant, as many features introduced for the purpose of the pandemic may have unintentional uses in a post-pandemic context.

6. **Scientific Efficacy and Validity:** Finally, not all tools are necessarily scientifically valid, or efficacious. Even when some tools may be scientifically validated, mere scientific validity is not tantamount to efficacy. For example, the science behind digital contact tracing may be sound, however, its efficacy has been questioned and debated in contrast to manual contact tracing efforts. Therefore, here, scientific validity has been interpreted in a narrower sense, to ascertain whether the tool works, and does what it claims. Efficacy on the other hand also examines the broader adequacy or effectiveness of these tools with respect to the overall public health measures and response to Covid-19.

The six parameters were divided into guiding questions in the following table.
Each tool was reviewed relying on news reports and developer websites to ascertain the function of the tool, technology used, development and deployment.

| Parameters | Guiding Questions |
|---|---|
| Equity and Inclusion | • What is the population that the tool covers; Are the tools accessible and usable by different sections of society? (Internet, language, etc.)<br>• [Incase of market based tool] Is the tool affordable?<br>• Could these tools be biased in any way? Could these tools potentially discriminate against any set of users? (Gender, class, race, ethnicity, and language)<br>• What are the additional steps required post the use of the tool for a user to receive medical assistance? |
| Privacy and Data Protection | • Does a privacy policy exist and is it openly available?<br>• Is there clarity on exactly what data is collected?<br>• Is there a restriction on who the data can be shared with?<br>• How is consent for the collection and sharing of data obtained?<br>• Is there a purpose limitation?<br>• What is the data retention period? |
| Accountability and Transparency | • What are the existing mechanisms of accountability in place?<br>Liability in case of false positives, technical failures (and the like)<br>Grievance redressal mechanisms?<br>• Are mechanisms of transparency extant throughout the lifecycle of the technology?<br>Are there processes of public consultation for the development of the tool?<br>Is information about the tool publicly available?<br>[in case of public sector apps] is the source code open? |
| Adequacy and legal frameworks | • What are the existing legal frameworks and regulations around particular technologies being used?<br>• Do the laws specifically address the technologies in question- are they updated? |
| Misuse | • Are the tools secure by design?<br>• Is function creep possible? In what way?<br>• What are the unintended consequences and potential societal harms that have not been accounted for? |
| Scientific Validity and Efficacy | • Are the tools scientifically validated and tested?<br>• What is the efficacy of these tools in the overall response to Covid-19? |

**Table 1:** Framework for reviewing responsible tech adoption in India during the Covid-19 pandemic.

# 4. Review of Tech Tools for Covid-19

# 4.1 Telemedicine

## *At a Glance*

- Telemedicine tools aim to enable medical professionals to provide remote healthcare and consultations to patients through information and communication technologies.

- We identified 6 telemedicine applications that provide Covid-19 specific services in India. Of these, 4 tools - DocsApp, Covid-19 Jagratha, MyDost and Wysa - have been reviewed, in-depth. However, this category of tools is much larger in terms of provision of telemedicine in general, which may or may not provide Covid-19 specific consultations.

- While telemedicine tools promise remote access and wider reach, lack of access to health infrastructure, internet services, and existing inequities limits the potential realisation of its promise. Even the basic requirement of a smartphone and internet access excludes a significant portion of the Indian population from these tools.

- The privacy guaranteed by telemedicine apps varies across cases - some tools (such as DocsApp and Covid-19 Jagratha) provide a privacy policy with weak measures for data sharing and liability. On the other hand, the privacy policy of tools such as Wysa have strong data privacy and security measures in place.

- These tools are governed by the new Telemedicine Guidelines, 2020. The guidelines specify necessary identity verification processes for both doctors and patients. However, they also mandate that the doctors maintain records of their patients without any clarity on the duration of data storage. Further, the guidelines do not enhance transparency and accountability of the telemedicine app provider.

- Examples of the successful application of telemedicine in India indicate that there is a need to combine online and offline processes such as setting up brick and mortar clinics with staff to assist in accessing telemedicine for the efficient application of these tools.

## What is it?

Telemedicine refers to the use of information and communication technologies in order to remotely deliver health diagnosis and treatment services. In the recently established Telemedicine guidelines, the Ministry of Health and Family Welfare (MoHFW) defines telemedicine as the "use of ICTs to exchange valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities".[13]

According to a report by telehealth services provider, Practo, there was a 500% rise in telehealth consultations in India, between March 1 to May 31, 2020, with 80% of users being first time users.[14] In addition to Practo, other leading telehealth providers in India such as DocsApp and Mfine have also witnessed increased purchase and investments. It has been reported that, propelled by the Covid-19 situation, India's healthtech sector is poised to become a $21 billion market by 2025.[15]

While the telemedicine service providers in India are aplenty, in our tracker we have identified/reviewed 6 telemedicine applications which provide Covid-19 specific services. For instance, DocsApp, one of the leading telehealth consultation providers in India, with services across 11 cities, has launched a Covid-19 risk assessment tool, that allows users to assess the chances of being affected by Covid through a series of questions, which then creates a risk-score based on symptoms. Through the platform, individuals can consult doctors who can then suggest whether a test is required.[16] Additionally, it also has a partnership with Phonepe where DocsApp is featured on its platform, enabling users to directly consult with doctors.[17] Other telehealth consultations catering to Covid-19 cases and other medical health cases, include Practo and MFine. In addition to commercial enterprises or private businesses in telehealth, some state governments in India have also deployed applications which provide teleconsulation services. For example, the Covid-19 Jagratha app, developed by NIC eGov, also provides teleconsultation services in addition to other services.

Further, teleconsultations for mental health have also witnessed a 200% spike during the past few months in India based on a report by Practo.[18] Applications such as YourDost and Wysa, are providing teleconsultations for people dealing with Covid-19 related stress and anxiety. In addition to the telemedicine sector, other

popular social media apps have also begun to add on services to cater to the mental health of users. For example, SnapChat recently rolled out a 'Here for You' feature which provides updates on safety and support for mental health in India.[19] While this feature is not a Covid-19 specific service, with many new users beginning to consider/use teleconsultations in India, a new market for mental health support services and tele-consultations seems to be opening up in India.

## How does it work?

Telemedicine uses ICTs to enable the provision of remote healthcare services by medical professionals. It offers patients a platform to request for consultations with a physician through various modes of communication; it requires patients to provide basic information on their condition based on which the consultation is scheduled. The physician is directly connected to the patient to carry out the consultation and assess next steps.

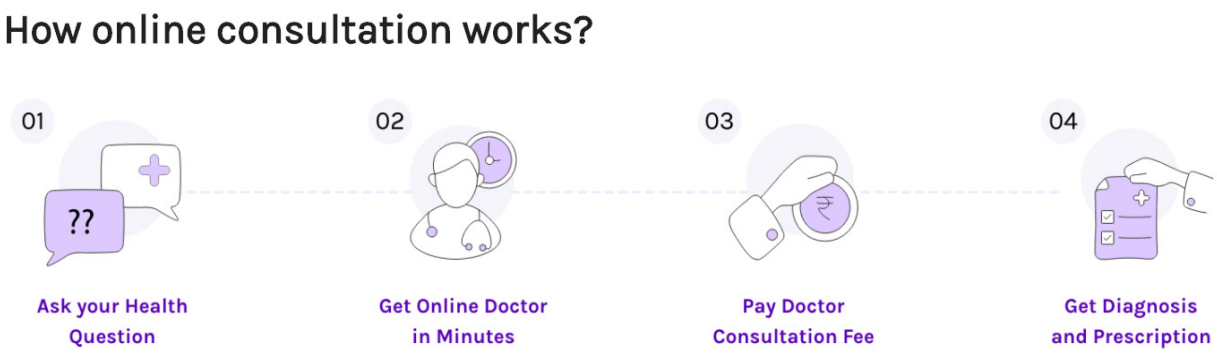


Figure 1: Image from *DocsApp*. Retrived August 10th, 2020.

## Rapid Review

Given the lack of access to quality healthcare, particularly in rural areas, telemedicine has the potential to provide access to healthcare across remote areas in India. However, for such a technological system to work, first order problems of access to infrastructure and internet connectivity as well as problems such as gender equality, and differential access to healthcare, digital literacy, and last mile connectivity need to be addressed.

**On equity and inclusion:** According to current estimates, about 500 million users in India use smartphones, of which 77% are online.[20] Thus, even the basic requirement of a smartphone and internet connection, leaves out more than half of India's population. None of the applications/tools reviewed in this category have been designed for feature phone users, and are also not likely to work for low bandwidth users.

Furthermore, for telemedicine to be accessible to all, it will require more than a smartphone and internet access. many Indians continue to be excluded from any formal or digital banking system; India had only 45 million active urban online banking users in June, 2017 according to a report by the Boston Consulting Group.[21] This creates another hurdle to access and pay for healthcare services online. Gender parity also plays a large role in India, both in terms of how healthcare is accessed as well as access to digital infrastructure and mobile phones. Research conducted by Harvard professor, S V Subramanian, shows that there is excessive gender bias when it comes to women's access to healthcare in India - with only 37% of women accessing health as compared to 67% men.[22]

Further, amongst reviewed tools, while the actual telehealth consultations between doctor and patient can be assumed to be provided in regional languages, the user interface of these tools vary in the number of languages they support. In the case of DocsApp, for instance, teleconsultations are available in 17 languages, however the app interface works in only two languages (Hindi and English).[23] Wysa, the AI chatbot for mental health, thus far only supports English language users, however, consultations can be in regional languages.[24] Covid-19 Jagratha appears to be available only in English based on images on the Google Appstore, however, its corresponding website does indicate that it might be available in Malayalam.[25]

**On privacy and data protection:** There are variations amongst different applications reviewed regarding the degree of privacy, anonymity and data security offered. For instance, Covid 19 Jagratha previously, Covid Care Kerala app, provides a basic privacy policy essentially informing the user that it cannot be held liable for information provided by the application. In the case of DocsApp, which does have a privacy policy in place, the terms of the policy are concerning. DocsApp,

for example, states that it 'cannot guarantee that the individual information won't be disclosed in a manner that is not covered by the policy.'[26] This indicates that the platform can retain and share data beyond the original purpose, and does not require additional consent from the user. This could lead to misuse of data and thus requires the introduction of mandatory regulations for data collection or legal frameworks that govern telemedicine applications.

Amongst the other tools reviewed, Wysa has a strong privacy and data security policy, clearly specifying that it does not collect personal information of users. The policy states that data is only shared with third parties for operations and analytics. No conversational, medical or psychological data is shared and in any event, data is encrypted. Further, there is a specific data retention period of 24 hours in case personal information is voluntarily shared on chat, after which such data is redacted. In the case of the YourDost app, the privacy policy provides very little information on data collection, sharing and retention. For many of these applications, very little information on the actual data security measures is available

**On accountability and transparency:** While the introduction of the Telemedicine Guidelines is a positive step towards legitimising the telemedicine sector, and brings a measure of accountability towards the doctor-patient communication over telemedicine applications, it does little to enhance the transparency and accountability of the tool or app providers. For instance, in DocsApp's terms and conditions, it very clearly maintains that it will not be held liable for any issues arising out of the consultation process between doctors and patients on their platform. Similarly, in the case of YourDost, the terms state that the platform will not be liable for any advice provided by its experts. This is due to the fact that some of the emerging services in this sector, such as YourDost and DocsApp, essentially act as platform aggregators, simply introducing clients with medical professionals.

In such a scenario, the rules and regulations regarding processing of data through aggregators mandated by Intermediary Guidelines under the IT Act, 2000, do apply to such platforms. However, the absence of wider systemic accountability means that aggregators have very little accountability regarding fraudulent actors or malpractice operating on these platforms. For instance, in the case of YourDost, we found the credentials of experts on the platform to be questionable, as they are not identified as medical professionals.

Further, problems of accountability and transparency are even more entrenched in the case of the Covid-19 Jagratha. Not only does the app bundle several types of services, from teleconsulations to grocery delivery, there is very little publicly available information on the legal safeguards and accountability measure adopted by the app, if any.

**On adequacy of legal frameworks:** While telemedicine has operated in the legal grey area for more than a decade in India, the New Telemedicine Guidelines released by the MoHFW set specific requirements for use. For instance, guidelines place much needed verification processes in place, whereby both patients and doctors/health professionals have to establish identity in the process of consultation.

Similarly, the guidelines also necessitate that a patient's personal data should not be disclosed without their written consent; this is also mandated by the IT Act, 2000, which is supported by the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.

However, one key concern with the guidelines that also overlaps with privacy issues, is that the guidelines mandate that doctors maintain records of their patients, without any clarity on the duration for which these need to be maintained.

**On misuse:** In the absence of adequate data protection measures and lax data security practices, both personal health data as well as metadata shared across some of these platforms could be potentially shared with insurance agencies. Additionally, even though the Telemedicine Guidelines address some of the concerns regarding unscrupulous practices, such as fraudulent medical practitioners on these platforms, there are limited means to confirm the adequacy of the verifications and enforcement of the guidelines in place.

**On scientific validity and efficacy:** Amongst the tools reviewed, only one application could be assessed on grounds of scientific validity - Wysa. There is no information on the DocsApp Covid-19 risk assessment tool and whether it is scientifically validated or in line with WHO, CDC or the Ministry of Health and Family Welfare guidelines.. In the case of Wysa, the app provides results on its validation and efficacy for multiple use cases. Further, it states that it is compliant with UK DCB 0129 Standard

of Clinical Safety standards.

In terms of efficacy, while telemedicine as a way of providing remote access to healthcare in the context of Covid-19 has seen increased uptake in India, as a service it is still only accessible to a small percentage of the Indian population. However, this is not to state that telemedicine is not effective in providing remote care, but that such measures need broader infrastructures in place. For instance, Aravind Eye Care which has been providing telehealth consultations and services for ophthalmology in India, has worked with various state governments to set-up rural service centres, where patients can go in order to be connected to health professionals online.[27] This can help bypass some of the literacy and access issues we covered in this section.

## 4.2 Remote Health Monitoring

### *At a Glance*

- Remote Health Monitoring tools and systems are designed to remotely monitor and track vital signs (heart rate, oxygen levels, body temperature, and respiration rate) of a patient.

- We identified 7 remote health monitoring tools aimed at providing healthcare for Covid-19 patients in India. Of these, 5 tools - MONAL, Indore 311, RayIoT, KARMI-BOT, and OXY 2 - have been reviewed in-depth.

- These systems are typically deployed in select hospitals or medical colleges. Some devices (such as RayIoT and Oxy 2) are also market-based and hence can be unaffordable to some parts of the population. State-mandated tools such as Indore-311, provides a pulse oximeter free of cost; however it requires the individual to have a smartphone to use the Indore-311 app to record the measured data.

- A few tools do not provide privacy policies, thereby failing to comply with the mandate that requires corporate bodies dealing with personal data to host privacy policies according to the Information Technology Rules. Some tools also grant access to unspecified individuals under the label of 'authorized persons' or 'affiliates and service providers'. Given that the tools measure and store sensitive health information, data privacy and data security measures are necessary safeguards.

- Liability in the case of technical failures or inaccuracies, accountability and transparency mechanisms were largely missing amongst the tools.

- Although remote health monitoring systems are generally accepted as a part of telemedicine, they are excluded from the new Telemedicine guidelines. Hence, they are only governed by the IT Act, 2000 and Rules which does not cover the extent of data privacy and security necessary for these systems.

- The tools raise concerns regarding the growing trend of somatic surveillance in the use of health tech. Given that the body becomes embedded in networks of data, it raises concerns of the data being misused for policing or by social sorting mechanisms.

- In terms of efficacy, these systems lack wider applicability due to cost, availability and prior infrastructural gaps. Current health infrastructure in India is grossly inadequate to roll out such technologies at a scale large enough to benefit the most vulnerable groups in society.

## What is it?

Remote health monitoring systems are a subset of telemedicine applications that uses a range of technological devices to monitor health and clinical signs of a patient remotely.[28]

In the context of Covid-19, remote health monitoring has emerged at one level as a useful solution which can help reduce exposure to Covid positive patients and limit risk of spread amongst healthcare providers and medical practitioners. In our tracker we have identified at least 7 remote health systems which are being used to administer healthcare to Covid-19 patients in India. For example, in Bangalore, Ramaiah Medical College has teamed up with Stasis Labs. In Delhi, researchers at BEL institute and AIIMS medical college have also developed.

## How does it work?

Remote monitoring systems work through a network of devices. Different types of sensors are used to monitor the corporeal and vital signs of a patient, such as heart rate, oxygen levels, skin temperature, which is then translated into data, which can be accessed in real time and analysed by doctors and nursing staff on their phones, or computers.

In our sample, remote monitoring systems include a variety of technological means that range from robotics to sensors to wearable devices. For example, Vincense is

a wearable device that measures vital signs (pulse rate, oxygen levels, temperature and respiration rate) and transmits the data to a secure cloud server. This data is stored in the cloud and is made accessible to healthcare providers for monitoring.

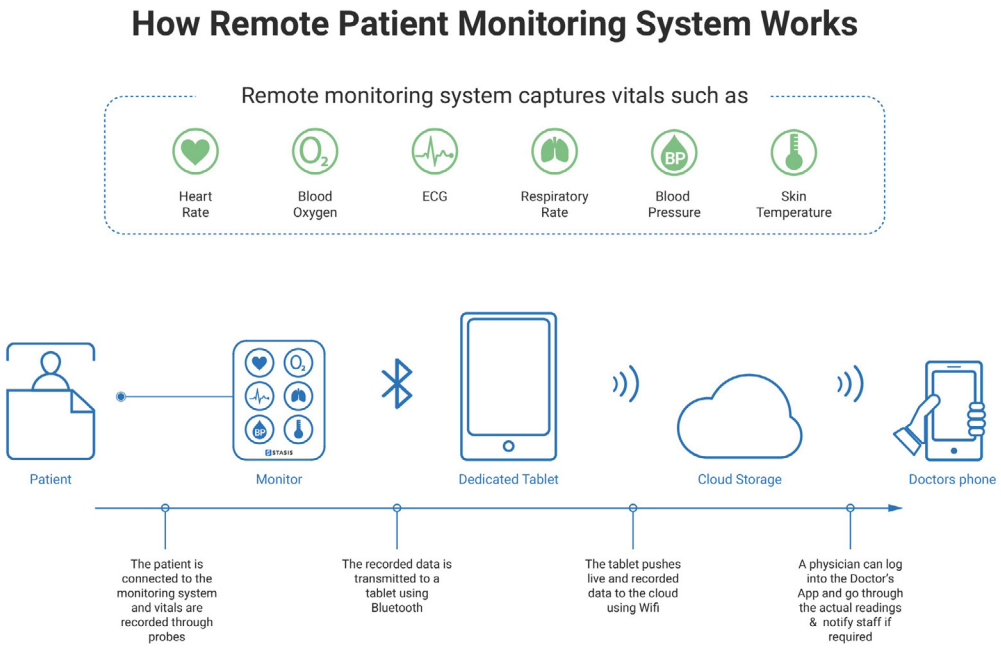


Figure 2: Image from *Stasis Labs.* Retrived August 18th, 2020.

## Rapid Review

Broadly, remote monitoring systems have the advantage of minimizing the risk of exposure and enabling continuous monitoring of patients, even outside of intensive care units (ICUs). Smaller and more portable systems, such as pulse oximeters which only measure oxygen levels can be used for self monitoring and tracking at used for home quarantine of those with milder symptoms, and can reduce the burden on hospitals.[29]

**On equity and inclusion:** Depending on the portability and infrastructural needs of these systems, these systems can either be used at home for self-monitoring or installed in hospitals. 5 out of the 7 systems we assessed are designed for hospital use only. One of these applications, Indore 311, has been developed by the State, is free of cost and patients are provided with free pulse oximeters provided by the state. However, for any of these systems to work internet connectivity is the baseline infrastructural requirement. Further, Indore 311 is only usable on smartphones,

thereby excluding a vast majority of feature phone users. From publicly available information, it appears that only a small fraction of private/ government hospitals have deployed these systems.

**On privacy and data protection:** Under the proposed PDP Bill, data collected from sensors and wearable devices under this category would be classified as sensitive health information. Currently, there is little clarity on the nature of data protection and privacy frameworks for these systems. While it can be assumed that similar to other patient monitoring systems such as ventilators, and based on descriptions of these systems on the company websites, the data collected through these systems will be accessed by medical health professionals and nursing staff, but there are no clear indications if there are any restrictions to access by others. In the case of Indore 311 for example, the privacy policy states that 'affiliates and service providers of Indore 311' will have access to data. Similarly, for Oxy 2, data is said to be uploaded to company servers and is accessible by only authorised persons but no further clarity on what is meant by authorised persons.

Aside from privacy, concerns also arise over data security measures of these systems. In April 2020, Interpol issued a 'purple notice' to all its 194 member countries, warning in its advisory: "Hospitals and other institutions on the front lines have also become targets of ransomware attacks designed to lock them out of their critical systems in an attempt to extort payments." Prior to the pandemic, lax cybersecurity measures in India, has resulted in the theft of healthcare data. In 2019, cyber criminals hacked a leading healthcare website in India and stole 68 lakh records of personally identifiable information regarding patients and doctors.[30]

**On accountability and transparency:** Amongst the reviewed tools, there was an overall lack of clarification regarding the accountability and transparency mechanisms adopted by the developer. Given that there are few legal regulations that govern Telehealth and telemedicine tools, the responsibility(liability) of tech companies and public participation is essential particularly when the tools have been deployed as a state-response.

Further, the importance of accountability is amplified when noting the pace at which these tools have been developed and launched. 4 out of the 7 tools under this category were primarily developed in response to the pandemic. Tools such as RayIoT and Karmi-BOT were developed by tech companies that were already

invested in medical tech solutions. Further, some pre-existing tools were also modified to fit the pandemic's context. The Indore 311 app, was initially developed as a platform for citizens to engage with civic authorities and raise local issues/ concerns. This was modified by adding a 'home isolation' feature which allows users to assess their vitals (using a pulse oximeter) and update them on the app for the IMA control room.[31]

In such cases of rapid-response tools, transparency in the process of deployment and use ensures that other parameters such as data privacy, efficacy, and potential misuse are taken into consideration before a widespread deployment. Since these tools are designed to record and collect information, it is also important for developers to clarify liability in the event of a technical failure or inaccurate capturing of vitals.

**On adequacy of legal frameworks:** Remote Health Monitoring in the medical field has been widely accepted to fall within the ambit of Telemedicine. The WHO's definition of Telemedicine points to it as the delivery of healthcare services, where distance is a critical factor by healthcare professionals using ICT for various specified medical purposes.[32] While remote health monitoring meets this definition in terms of its functionality, the newly introduced Telemedicine Guidelines appears to exclude it from its application. The guidelines primarily focus on the provision of consultations through telemedicine, a service that is not provided by any of the tools reviewed under the remote health monitoring category. Although the introduction of these guidelines was a step in the right direction, its exclusion of remote health monitoring continues to leave gaps in the provision of adequate regulation.

The IT Act 2000 continue to regulate the use of any personal data collected by the tools. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 sets out certain security procedures and practices that need to be adhered to while collecting/processing sensitive or personal information, which is very limited in its scope including only physical, physiological and mental health conditions, medical records and history specifically within health data. Additionally, the law only necessitates consent as a prerequisite for collection and processing.[33]

An important point to note in this category is the lack of privacy policies in place for a few tools; this a direct failure to comply with the mandate on corporate bodies that deal with personal data to provide a privacy policy.[34]

**On misuse:** Remote Health Monitoring systems, in medical praxis is a way to track symptom progress of patients. However, in the context of Covid, some of these systems have also acquired policing functions. For instance, both the Indore 311 system and Oxy 2 integrated geofencing functions, which alert 'authorities' of patients movements.

Further, research on the emergence of wearable devices and the quantification of health, invoke a growing trend towards new forms of 'somatic surveillance' - which refers to the increasingly invasive technological monitoring of and intervention into body functions.[35] While remote health monitoring systems offer 24/7 monitoring of patients and augmenting lack of medical staff, as benefits, scholars have raised concerns over the emerging culture of surveillance in the use of health tech through which the corporeal body becomes embedded in an information network. Once integrated into such networks of data, misuse of this data through social sorting mechanisms such as by insurance companies pose a real problem.

To add, the quantification and networking of the body into architectures of information have the potential to widen the divide between the digital haves and have nots. While there are questions of access, data protection, privacy and security, equally concerning are the issues of exclusion.

**On scientific validity and efficacy:** The integration of AI and other data analytics which are used to provide analysed information to medical practitioners, necessitates testing of the validity and accuracy of such information. Amongst the systems assessed, RayIoT devices claim an accuracy of 98% in clinical settings. Similar information is not available regarding other devices in this category.

In terms of efficacy, these systems lack wider applicability due to cost, availability and prior infrastructural gaps. Thus, even though these tools can minimize risk of exposure and provide better monitoring of patients, factors such as cost, and inequitable access in India does not make them effective in combating Covid-19. Current health infrastructure in India is grossly inadequate to roll out such technologies at a scale large enough to benefit the most vulnerable groups in society.

## 4.3 Testing and Screening

### *At a Glance*

- Testing and Screening tools aim to test and screen individuals for Covid-19 symptoms to ascertain need for further medical interventions.

- We have identified 10 testing and screening tools for Covid-19 in India. Of these, 4 tools - JARVIS, HealthifyMe, AyuSynk, and Test Yourself (Goa and Puducherry) - have been reviewed, in-depth.

- Similar to previous categories, equity and inclusion remains a concern. While there are a broad range of applications and diverse technology providers in this category, equitable adoption is blocked due to lack of access to internet services and infrastructure.

- The privacy policies of all the reviewed testing and screening tools have been available and largely detailed around the data collected. However, there are significant gaps around purpose limitation and data retention periods for all the tools. Since most have been developed by the private sector, there is little clarity over the nature of data sharing and data ownership.

- There is a continuing lack of information around the accountability and transparency mechanisms in place.

- Possibilities of misuse are largely dependent on the type of technology used. For example, an AI-powered testing and screening tool could potentially be misused as a tool for policing.

- There is little to no evidence on the scientific validity of these tools. While they may be efficacious substitutes, the high cost of technology, lack of data protection frameworks, and concerns regarding misuse are important issues to be addressed.

## What is it?

Due to a shortage of testing kits in the initial phase of Covid-19,[36] and a general lack of public health infrastructure in India for testing;[37] several tech companies in India have begun trying out novel methods to triage and screen Covid-19 positive patients.

In our sample, we have identified 10 tech tools which are being used for testing and screening purposes. The purpose of this category of tools is to apply novel methods including AI based sound detection, image recognition and temperature detection in order to detect Covid-19 symptoms and cases. For example, Jarvis (short for Joint AI Research For Video Instances And Streams) is a tool developed by Staqu, which uses AI powered thermal cameras to detect body temperature/heat signature. It has been proposed as a disease surveillance tool for public areas. While there is little information on the scale of adoption of this tool, reports suggest that it is being used in Staqu's own offices. Other examples for triage tools include the Cough against Covid project, which is being developed by Wadhwani AI and Stanford University.

Some tools in this category are also those which have been developed to enable safe testing. Meaning, while lab tests such as RT-PCR tests are used, these tools facilitate the testing in a exposure less manner. For example, Pulse Active Network Station has set up 'smart health' kiosks for which use a network of connected sensors to produce a report on 21 body parameters to test for comorbidities. Although originally designed to test for lifestyle diseases, it has now been retooled as a swab collection kiosk, which will also provide comorbidity analysis to the Telangana government.[38]

Further, in our research, we have also identified screening tools that have been designed to aid self-assessment for Covid-19. For instance, one of the apps in this category which has been developed by the State government of Goa in partnership with Innovacer, a San-Francisco healthcare technology company firm. It uses an online survey form taking in details such as location, travel history, comorbidities and health history to recommend testing and quarantine for individuals. Similarly, Healthifyme, a leading health and fitness application in India, has developed an Immunity Assessment Test on its app to help users assess their immunity. The test includes questions on the users age, diet, workout and sleep regiment, smoking habits and medical conditions.

## How does it work?

The lab testing process for Covid-19 detection used a reverse transcription-polymerase chain reaction (RT-PCR) process, which is applied to nasal swab samples collected from patients.

In lieu of this, the tools being developed for testing and screening essentially utilise different technological means (such as image recognition, thermal imaging) which uses proxy parameters such as cough sounds, body temperature, and CT scans to detect the presence/absence of Covid-19.

In the case of cough sounds, AI algorithms are trained to distinguish between different respiratory sounds - those which indicate Covid-19 and those that do not. Through a mobile application, a user can upload their respiratory sounds, which will then be algorithmically processed to identify possible Covid-19 infections. Similarly in the case of thermal scanning, if the algorithm picks up a spike in temperature, it can inform either the individual or public authorities based on who has deployed the technology and in what institutional setting.

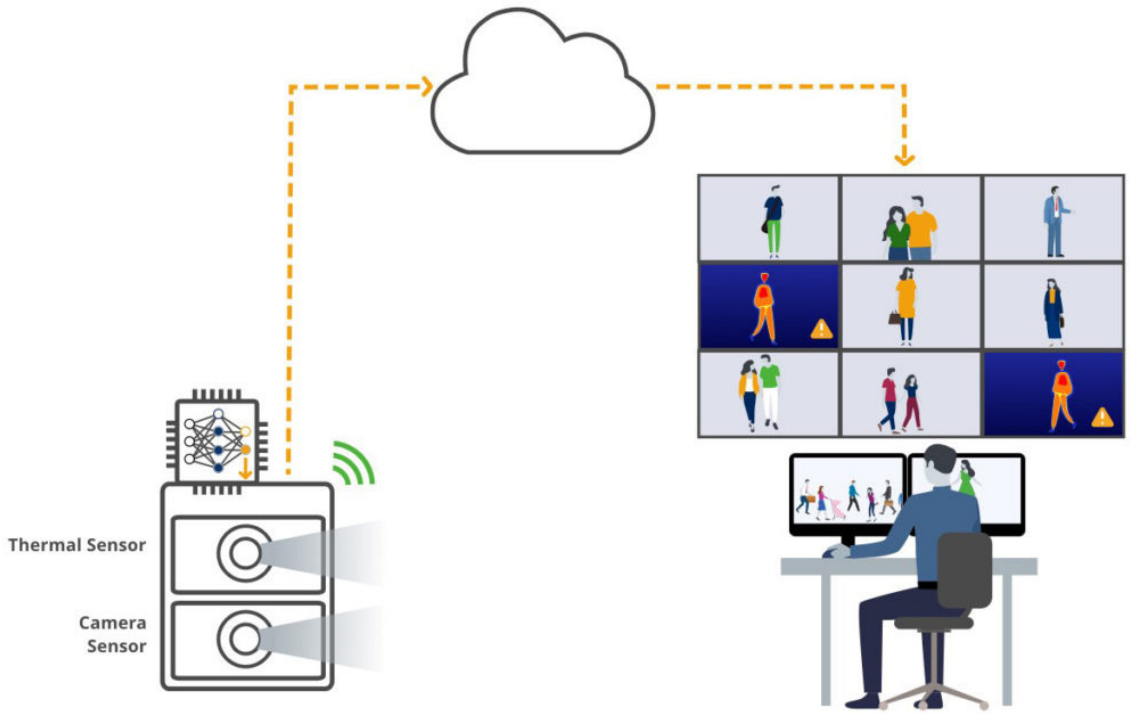


Figure 3: Image from *AnyConnect Academy*. Retrived August 18th, 2020.

In some other instances, chest X-rays are being used as proxies instead of respiratory sounds. With shortages and delays in PCR tests, chest X-rays had become one of the fastest and most affordable ways for doctors to triage patients. The X-rays enable detection of Covid-induced pneumonia, and AI is used to speed up the process of detection.

The self assessment tools identified in this category utilize statistical models to assign degrees of risk for potential Covid infection based on a number of parameters. Example, Testyourself app is based on CDC guidelines, and takes into account self-reported factors such illness severity, and risk factors like age and pre-existing conditions.

## Rapid Review

In the absence of widespread lab testing, these applications can be a way to augment existing capacity and reduce the burden on hospitals and medical staff through prior screening. However, some of the tools in this category are still in development, whereas others raise concerns regarding misuse and efficacy.

**On equity and inclusion:** Many of these tools are being developed by the private sector companies and therefore will come at a cost. A crumbling public health infrastructure in India, is already plagued with issues of equity and access and therefore the same applies to most of these tools. However, in the case of state deployed tools such as the TestYourself app, cost is not a limiting factor, however, it still requires internet connection to work.

**On privacy and data protection:** With most of these tools being developed by private companies, questions of privacy and security of data become more pertinent. Like remote health monitoring devices, the data collected by such tools can be quite granular, and relates to not just personal information, but bodily/corporeal information.

As is the case with most tools that have cropped up as a response to the pandemic, the privacy policies of testing and screening tools are loosely worded for the most part. For example in the case of AyuSynk, which allows for the storage of

respiratory sounds of patients as part of their health record, there is no clarity on the granularity of data which is collected. Their privacy policy indicates that basic personal information is collected by the device but not limited to data required for device use.

Further questions arise over the nature of data sharing agreements between government agencies and private companies. There is very little publicly available information on the data sharing agreements between the two. For instance, the TestYourself app, which has been developed by a U.S based private company called Innovaccer, the search for a privacy policy redirects the user to Innovaccer's privacy policy. This not only raises questions about data sharing but also the ownership of data.

**On accountability and transparency:** The continuing lack of information around the functioning of many of the categories of tools, particularly within this parameter, have left only assumptions that there are largely no mechanisms in place. As tools vary in nature, an example to distinguish the manner of functioning is the mobile application HealthifyMe - a health and fitness based app that has developed an immunity assessment test which is essentially a series of questions posed to the user to determine immunity to Covid-19. This test is likely to have no accountability or transparency embedded in it apart from the human element that initially developed the test.

**On adequacy of legal frameworks:** The only relevant regulation appears to be the Information Technology Act, 2000 in the absence of a comprehensive data protection framework to regulate the collection and processing of any personal data. However, as some tools possess technology such as AI, there is currently no legislation in place to provide guidelines or safeguards.

**On misuse:** The possibilities of misuse are wide ranging dependant on the type of technology deployed by the tool; for example, JARVIS involves AI-powered automated screening through a thermal camera which raises concerns around the likelihood of its use for policing and even inaccuracies that might lead to either misdiagnosis, dictating behaviour (if deployed in office spaces) and possibly discrimination.

**On scientific accuracy and efficacy:** In some instances, such as Wadhwani AI's cough against Covid, the tools are still in development and therefore figures on accuracy and validity have not yet been released. However, amongst those which have been deployed, there is little evidence on the science behind these tools. For example, the HealthifyMe tool which provides an immunity score to individuals, there is no clarity on the accuracy of the assessment test or the score that it creates. Similarly, there is no publicly available information on the degree of accuracy in case of Jarvis.

While these tools are potentially efficacious substitutes for swab testing, the high cost of technology, lack of data protection frameworks, and concerns regarding misuse for surveillance calls for greater precaution and care in the deployment of these tools.

# 4.4 Virus Mapping and Contact Tracing

## *At a Glance*

- Virus mapping and contact tracing tools are used to track the spread of the disease by identifying and monitoring individuals who may have been exposed to the virus.

- We have identified 6 virus mapping and contact tracing tools in India, of which 4 tools have been reviewed in-depth. These include: Aiisma (Aii Health), Sandhane, Covid Monitoring System, and Aarogya Setu - the official contact tracing app for India.

- The mandatory installation of contact tracing apps to travel and access workspaces discriminates against those who are not internet users, and those who do not own smartphones. Similarly, tools that assist with manual contact tracing are unfamiliar to those the tool is intended for, ASHA workers.

- There is no clarity on data privacy and security measures. Given that these tools are being made mandatory (for travel, to enter workspaces, housing societies, courts etc.), there is also no clear process of obtaining informed consent for the collection and storage of data. Concerns have been raised regarding India's official contact tracing app - Aarogya Setu - and its collection of excessive data, beyond what is required for contact tracing.

- There are currently no mechanisms of accountability for most virus mapping and contact-tracing applications. Since the possibility of inaccuracies is highly likely, it is particularly important to ensure liability of any technical failures.

- These tools are currently governed by the Information Technology Act and Rules. However, they are inadequate particularly in this case, as it does not include location data as sensitive personal data.

- The lack of updated legal frameworks and regulations also results in the high possibility of misuse by users or authorities. The possibility of function creep has been identified as a significant concern as these tools often combine quarantine management and policing as their secondary functions.

- The efficacy of the contact tracing method is dependent on at least half the state's population being traced and tested. Therefore, in its current form, the tools under this category may not be an effective method to contain the spread of the virus.

## What is it?

Contact tracing is a method used by health officials and epidemiologists, to identify, track and monitor people who may have been exposed to a disease, so as to manage their movement and prevent transmission.

Typically contact tracing is carried out manually and involves case investigation, of interviewing infected persons, to identify others who they may have come in contact with. Once identified, these people are notified of the potential risk and referred for testing.[39] Repeating this process, enables health workers to identify a 'spider web of transmission' of the disease and allows them to contain the spread of the virus. In the context of Covid-19, digital contact tracing applications have been developed in addition to applications that assist manual contact tracing practices.

In addition to Aarogya Setu, India's official contact tracing app, we have identified 6 mobile applications which are facilitating contact tracing in India, during the pandemic. These applications rely on users sharing their personal information which is geo-tagged for the purpose of tracing. In addition to contact tracing, these tools may also generate mobility trends, and hotspot mapping in order to allow predictive management of the pandemic and streamline resources.

## How does it work?

Digital contact tracing works through the exchange of data between different devices, through the use of bluetooth signals. In the process, digital contact tracing uses devices carried by people, such as smartphones, as proxies for people.
This data is analysed by 'a risk-scoring algorithm according to certain parameters (such as length of contact and number of contacts with persons reported to be infected with the virus, on the basis of either self-reported or verified testing data) to determine whether a user or public health authorities should be alerted about potential contact and what action should then be taken'.[40]

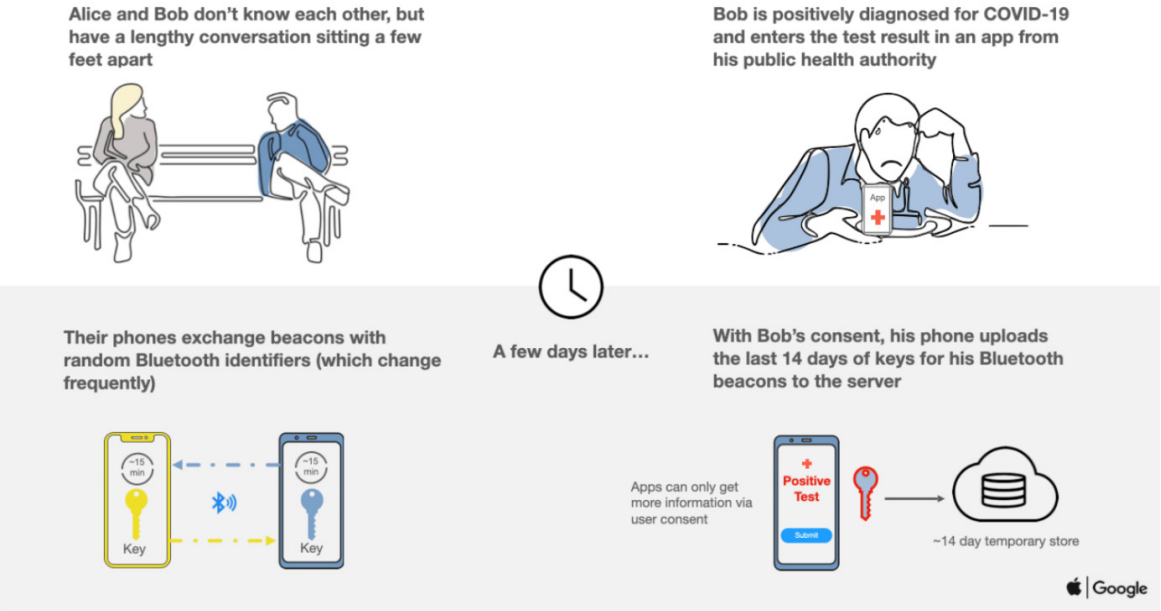


Figure 4: Image from *Apple-Google's Contact Tracing* Retrived August 18th, 2020.

## Rapid Review

In the context of Covid-19, the tech community has been swift in coming up with digital contact tracing solutions, which could either supplement or automate manual contact tracing. In the absence of ubiquitous testing, proponents of digital contact tracing could work better in slowing spread of the virus than traditional methods which combine intensive testing, with manual contact tracing.

**On equity and inclusion:** Digital contact tracing at the very least requires a smartphone. In India, over half the population (560 million) are not internet users and an even smaller section (354 million) own smartphones, thereby, excluding a majority of the population from digital contact tracing apps.[41] The exclusion of this population is particularly significant since there has been a push for the mandatory use of digital contact tracing apps. For example, passengers are required to install contact tracing apps to be eligible for domestic air travel. Indigo Airlines has listed a state-wise breakdown of quarantine regulations and passenger obligations.[42] In most cases, the installation of a specific contact tracing app (largely, Aarogya Setu) has been made mandatory by various state governments. This discriminates against a significant portion of the population that may opt for airline travel but do not have access to smartphones.

In the case of apps that assist manual contact tracing, the intended users are ASHA workers and Anganwadi workers. They are required to carry out door-to-door surveys using the apps to record data. In this case, accessibility is dependent on the familiarity and comfort of the workers using these applications. In Bengaluru, the city administration reported that ASHA workers did not prefer to input the data on the state's official contact-tracing app and instead carried out manual contact tracing in a format that was familiar to them.[43]

**On privacy and data protection:** There are many privacy concerns with regard to contact tracing apps that have not been significantly addressed by authorities that mandate the use of contact tracing apps. In most cases, there are no specific privacy policies or terms and conditions for the tool, to provide clarity on what data is collected, restrictions on sharing, purpose of storing and data retention periods. There is also no clear process of obtaining consent for the collection and storage of data.

Despite having a specific privacy policy and terms of service, Aarogya Setu has raised significant privacy concerns in India. One of the main concerns, raised by legal advocates and privacy scholars, is the excessive data collected by the app - which is not required for the purpose of contact tracing. This has attracted focus and attention since the app is endorsed by the government and is also the most installed contact tracing app in the world.[44] It has also been made mandatory for travel,[45] entering premises of private companies, and even legal institutions.[46] This

further complicates the informed consent of users who may be forced to provide consent in order to travel, work or seek legal recourse.

**On accountability and transparency:** There are currently no mechanisms of accountability for most virus mapping and contact-tracing applications. Since these tools are known to be inaccurate, it is particularly important to ensure liability in the case of any technical failures. In response to such critiques, the government made Aarogya Setu an open-source app. This means the source code is available for researchers/developers to examine and identify loopholes and flaws. However, it was soon discovered that the open source code only shows the interaction of the app with the user, and does not reveal the source code at the server end. The government does, however, clarify their liability in case of 'unauthorised access to user's information' in the Terms of Service for Aarogya Setu.

**On adequacy of legal frameworks:** With no legislative framework in place to govern the use of personal data for the purposes of contact tracing, protections provided fall to the current IT Act, 2000. However, the current regulations are grossly inadequate especially as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 does not include location data within its definition of sensitive personal data.

**On misuse:** Given the lack of legal frameworks and regulations that govern contact tracing apps, there is high potential for misuse by users, authorities, and external agencies. The most likely way misuse would play out in context of virus mapping and contact tracing apps is function creep. Most contact tracing apps do not limit or clarify the collection and usage of data. Secondary functions of quarantine management and policing often overlap with the original purpose of contact tracing. In the case of Aarogya Setu, the updated privacy policy (on May 24th, 2020) states additional functions of the app including - the display of government issued ePasses and other 'convenience services'.

Further, the mandatory use of contact tracing apps such as Aarogya Setu and Sandhane, to access essential services and spaces, discriminates against those who cannot use the app (or those choosing to opt-out). In addition to exclusion, the use of Aarogya Setu has been mandated by employers, housing societies[47] and police departments in certain places.[48]

**On scientific efficacy and validity:** The efficacy of contact tracing, in containing the spread of the virus, is largely dependent on the number of people that are being traced and tested.[49] Studies show that for digital contact tracing to be effective, at least 50% of the state's population needs to use the app.[50] Hence, the method of contact tracing itself needs to be reexamined as a primary response to the pandemic. Resources and efforts can instead be redirected to improving health infrastructure and increased testing.

On the other hand, apps that assist in manual contact tracing are primarily focused on digitizing and aggregating data. As mentioned above, these apps have already proven to be ineffective in the process of manual contact tracing, due to its in-accessibility by ASHA workers. Hence, the intended purpose is not served as all the data collected by the workers is not entered on the app.

# 4.5 Information and Alerts

## *At a Glance*

- Given the infodemic regarding the Covid-19 virus, information and alerts applications have been developed to provide citizens with verified information regarding official guidelines, health advisories, and helpline numbers. They may also provide updated Coronavirus-related statistics and mapping of containment zones in the city.

- We have identified 23 Information and Alerts applications in India. Of these, 5 apps - Cova Punjab, Delhi Corona, KSP Clear Pass, Dasoha, T Covid-19 - were reviewed in-depth.

- The tools in this category are primarily developed or deployed by state governments. Hence, they are intended to be accessible to all. However, these applications have been developed only for smartphones, and require internet access and connectivity for use. Further, many have been largely made available in two languages - the state language and English. This excludes communities in the state that are not native to the state.

- The applications raise significant privacy concerns as they collect excessive user data (device and personal) with no restrictions on data retention or purpose limitation. The privacy policy exists for most applications, however they are found to be written in broad strokes and refer users to the terms and conditions of the service provider. This does not place any liability on the state despite the applications being developed/deployed by the state.

- These tools are governed by the IT Act, 2000 and Rules. However, the collection and processing of personal data remains broadly unregulated by the IT Act, 2000, as well as the lack of data security measures specified in the privacy policy.

- The likelihood of inaccurate information on the app necessitates accountability mechanisms. However, there are no measures of grievance redressal or liability. State-backed apps also need to be transparent in their working. To this end, Aarogya Setu has partially made its source code open. However, other state apps have not done the same.

- The lack of a sunset clause in most applications raises serious concerns regarding the potential for misuse, particularly in a post-pandemic context. In some cases, the apps have been found to send alerts despite deletion from the device.

- The efficacy of such applications can be assessed based on the accuracy and legitimacy of the information provided by the apps. Some apps, for instance, have failed to update the real-time numbers of hospital beds available, resulting in a crisis for the hospital authorities as well as individuals in need.

## What is it?

The Covid-19 pandemic has also been accompanied by an infodemic regarding the virus, its origin, spread and containment. In order to provide verified and correct information, many state governments have developed official Covid response mobile applications, which provide citizens with information regarding Covid-19 in respective states.

The types of information provided by these apps include official guidelines, health advisory, helpline numbers, list of hospitals (for Covid testing). It may also include updated mapping of containment zones in the city.

We have identified a total of 23 different applications which serve as platforms for information and communication channels between government and citizens, which in some cases also includes volunteers and health workers. These include applications that provide self assessment tests such as T Covid-19, grocery delivery services such as COVA Punjab (Corona Virus Alert) App, teleconsultation services such as Covid-19 Andhra Pradesh, ayurvedic treatments such as Ayush Kavach, and others.

For instance, COVA Punjab (Corona Virus Alert) App, which has been developed by the Government of Punjab, provides citizens with preventive care information and other government advisories. While the provision of information and alerts is one of the key functions of many state backed applications, they can also include a range of other functions. In addition it also provides medical information, coronavirus-related statistics and updates, travelling instructions, locations and contact information of public hospitals in Punjab, a questionnaire for self-screening of symptoms, facilitates the reporting of unlawful assemblies, and a feature to request delivery of groceries in the time of lockdown.

The Delhi Corona App, developed by the Government of NCT of Delhi contains a self-assessment tool, guidelines and important helplines to ensure well being of the users. The app also allows the user to view all Covid-19 centers and access lockdown services like ration, e-pass and hunger/shelter relief centres. The stated goal of the app is to provide 'real time information on the number of hospital beds — both in private and government hospitals — available at any given time.

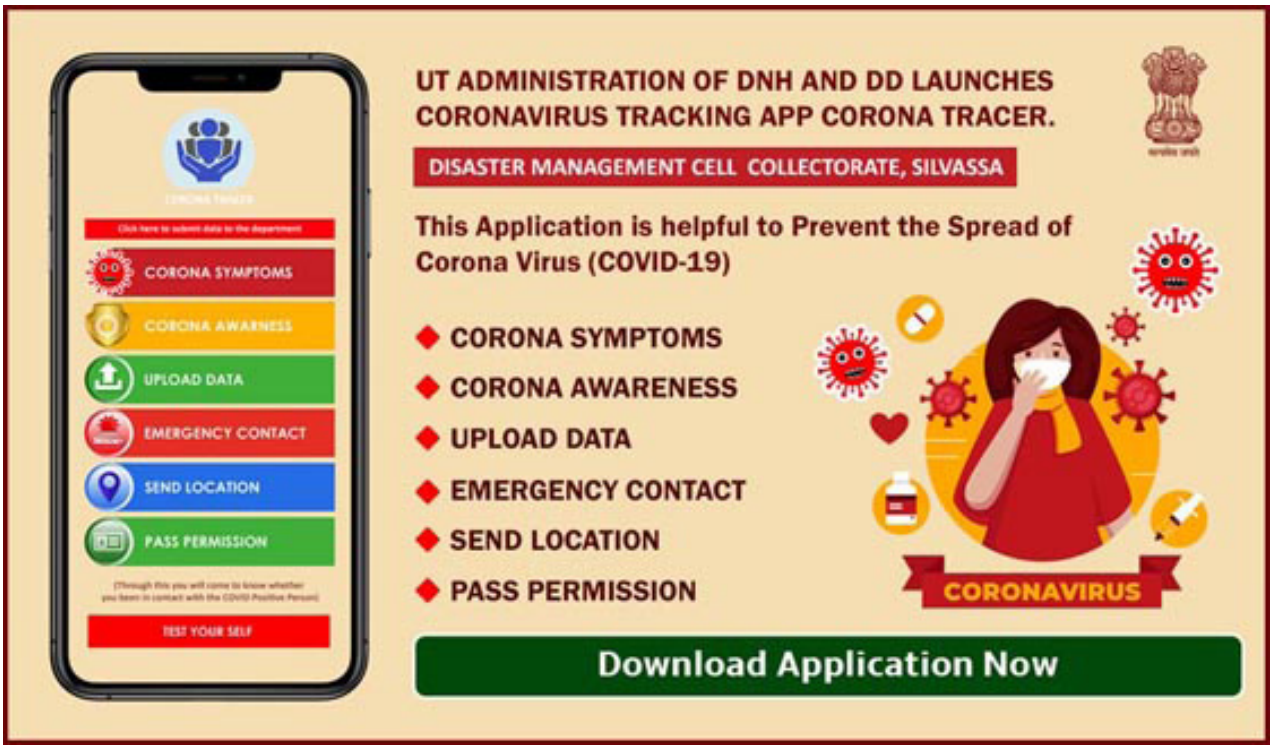


Figure 5: Image from *Dadra and Nagar Haveli District Administration.* Retrived August 18th, 2020.

## How does it work?

The applications present users with information by coordinating with multiple stakeholders. The Delhi Corona application, for example, collects data from hospitals across the city on the number of available beds, collates it, and presents it to users on the app. Other applications like COVA Punjab are actively updated to provide users access to advisories released by the government and also let them view coronavirus-related statistics and updates.

## Rapid Review

**On equality and inclusion:** Because most of the tools in this category are primarily state led, they are essentially free and can be used by anyone residing in the state or with phone numbers registered in the particular area-circle. However, none of these applications are designed to work for feature phones, and need internet access and connectivity for use. Further, while a majority of the applications support more than one languages, corresponding to the state, these in some instances ignore the multi-lingual and metropolitan characteristics of cities. For instance, the Delhi Corona App supports two languages - Hindi and English, even though a large number of other linguistic communities reside in the city.

**On privacy and data protection:** For several applications, privacy policy exists, however, these policies are often written in broad strokes and do not specify any data retention period, or restrictions on its use. Further, these applications collect a range of information from device data (Internet Protocol ("IP") address, device name, operating system version, the configuration of the app when utilizing our Service, the time and date of your use of the Service, and other statistics) to PII including name and location. In case of epass applications, vehicle registration number and Aadhaar number are also required (KSP clear pass). These applications also in some instances provide access to third party service providers and share information with law enforcement agencies and other government departments. In cases where third party service providers are given access, the privacy policy simply suggests that the user refer to the privacy policies of these service providers. Broadly, these privacy policies do not place any real liability on the state. Further, some of the applications which are deployed by the state have also outsourced the development of these apps to third party developers and private companies (e.g. NMC Covid19 App).

**On accountability and transparency:** There is very little accountability and transparency mechanisms in place with regard to these applications. While the Aarogya Setu app has set a benchmark for accountability by opening up its source code, however, other state backed applications have not done the same. Further, many of these applications have been developed in partnership with private, local vendors. It is not clear what sort of procurement standards were applied before contracting vendors.

Further, in the case of the Delhi Corona app, which claims to have been designed as a way to ensure accountability from hospitals and medical centres in Delhi by keeping tabs on the number of beds available. However, there are little to no accountability mechanisms in place for the app itself, with several users and hospitals complaining about inaccurate information on the app.

**On adequacy of legal frameworks:** As the Personal Data Protection Bill is still yet to become legislation, there are no applicable legal safeguards in place; even if PDP were to be passed, it still gives broad exemptions to the state. The tools therefore continue to fall within the ambit of the IT Act and its Rules but fail to specify in their privacy policies, the security measures or procedures in place for its collection and processing of personal data. This is a requirement mandated by the legal frameworks in place.[51]

**On misuse:** The integration of these applications into the 'new normal' of Covid-19 can be very hard to peel back in the future. Since most of these apps do not have a sunset clause, and in some cases, the apps continue to send alerts even after deletion, this raises concerns regarding background running of these apps even post deletion by the user. Secondly, the absence of openness and transparency, creates a potential for misuse without citizen knowledge and consent.

**On scientific accuracy and efficacy:** In case of information and alert applications, scientific validity is not a factor of analysis. However, in terms of efficacy, many of these applications do not achieve what is claimed - primarily the provision of real time information. For example, information provided by Delhi Corona App on the number of hospital beds has been contested by hospitals in question, stating that even after repeated intimation by hospital staff, no of beds has not been changed on the app. Similarly, apps like Ayush Kavach in UP, developed by StuCare Technologies

and launched by AYUSH Department Government Of Uttar Pradesh, to provide updates for a healthy lifestyle, Immunity Boosting measures based on locally and easily available natural resources in Uttar Pradesh, etc. raises concerns regarding the efficacy and validity of such solutions for Covid-19.

# 4.6 Location Tracking and Quarantine Management

## *At a Glance*

- Location tracking and quarantine management tools are mobile applications that help authorities monitor the movements of individuals who are required to isolate themselves to prevent the spread of the virus. Most tools in this category are deployed by the state, as they are intended to enforce quarantine norms.

- We identified 23 applications under this category. Of these, 4 applications - GCC - Corona Monitoring, Intugine's Location Intelligence Platform, SMC Covid-19 Tracker, and Saiyam have been reviewed in-depth.

- Given that these applications require a smartphone, they are made inaccessible to individuals that may not own smartphones.

- The applications collect excessive data and have weak data privacy and security measures in place. Most of them lack a privacy policy, and those that have them in place are written in broad strokes.

- These applications are governed by the Information Technology Act, 2000. Although this regulates some aspects of data protection - a large portion of personal data that is collected remains unregulated.

- Transparency and accountability mechanisms required for applications developed such as open source codes and grievance redressal mechanisms are missing. Additionally, there is very little information publicly available regarding the working of the applications.

- Function creep is highly likely in the case of location tracking apps. Given that they collect personal data for the purpose of policing (with no restrictions on the purpose of data collection and storage) - the surveillance of individuals by state governments is a potential misuse of such applications.

- The efficacy of such tools has been observed to be faulty. Incorrect tracking and reporting of data has led to multiple instances of individuals falsely being labeled as offenders.

## What is it?

Location tracking and quarantine management tools are technological solutions designed to help authorities monitor and track the movements of individuals who are required to isolate themselves to stop the spread of the disease. Unlike digital contact tracing, location tracking and quarantine management tools, these tools have not been developed to trace contagion from one person to another. Instead, these tools have an enforcement function, and are used as attendance mechanisms to ensure individual compliance with quarantine and other directives.

All the tools under this category are mobile applications designed to track individuals and enforce quarantine norms. Save for one application, all were either developed by a state government or developed by a private company and deployed in partnership with a state government.

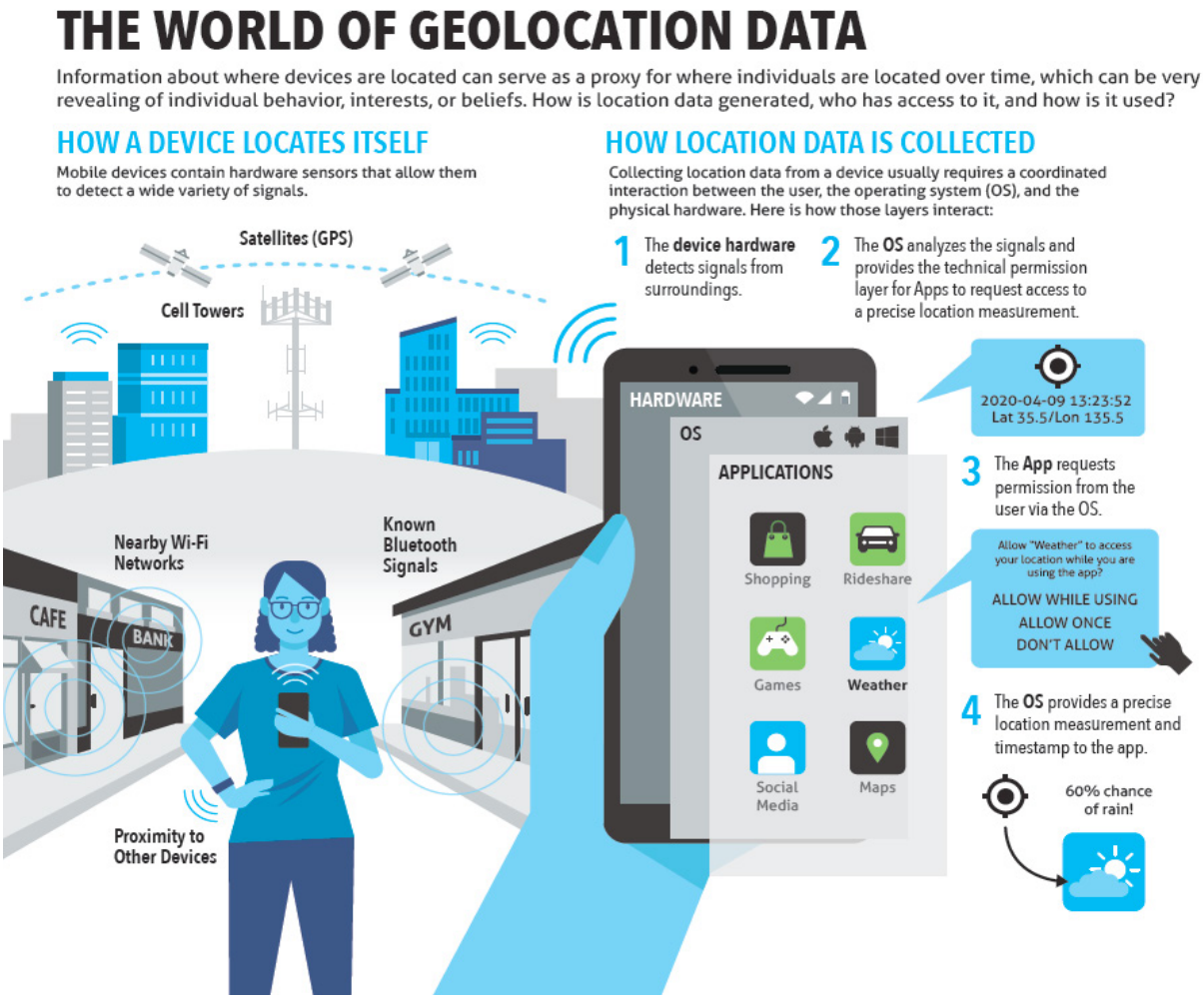


Figure 5: Image from *Future of Privacy Forum.* Retrived August 18th, 2020.

In addition to location tracking functions, some of these tools also incorporate wider functions that allow public authorities to manage people's movements, quarantine restrictions and state response - through the creation of dashboards

## How does it work?

As a world-wide response to the pandemic, several location tracking and quarantine management systems and applications have been developed to allow authorities to track citizen mobility in order to curb the spread of the virus. Unlike contact tracing, which aims to map the spread of the virus and ascertain which individuals might have contracted the virus, these tools are seen as a way to monitor and enforce restrictions imposed upon individuals required to quarantine themselves.

Since all of these tools are smartphone applications, they use a host of different technologies to monitor and restrict the movements of individuals, ranging from cell tower triangulation and GPS signals to geofencing and selfie attendance.

## Rapid Review

**On equity and inclusion:** All tools in this category are mobile applications developed to track the locations of users through mobile devices. This poses a challenge for governments as this approach doesn't cover individuals with feature phones, a sizeable chunk of the Indian population.

**On privacy and data protection:** A lot of these tools are developed by private companies, with various kinds of data being collected, shared, and used by them, all with either lackluster privacy policies, or no privacy policies at all. Most tools collect more information than they require, share them with third parties, and have no clear data retention policies.

**On accountability and transparency:** In spite of the fact that all but one application in this category was either developed like in the case of Chennai's GCC Corona Monitoring mobile application  or the deployment of SAIYAM by the Maharashtrian

state government, none of the applications have any known form of transparency or accountability mechanisms such as open source codes and grievance redressal mechanisms. Neither is sufficient information about the tools available, nor are their workings known to the public.

**On adequacy of legal frameworks:** While some provisions of the IT Act, 2000 cover certain aspects of data protection, they provide little to no protection to individuals' personal data that most applications collect. The PDP Bill contains broad safeguards, which while lacking in certain aspects, would still be better than the status quo. However, since the bill is not law yet, and the extant law barely contains any safeguards, the current legal framework is largely inadequate.

**On misuse:** Given the permissions they require, the data they collect, and the functions they serve, the expansion of the scope of these tools is not only possible, but highly likely. Most of these tools are not brought into existence with a restriction on purpose or any such sort of limitation.

**On scientific accuracy and efficacy:** These tools rely on location tracking technologies and the internet, a combination that can often lead to incorrect reporting of violations. There have been multiple instances of individuals being labeled as offenders having violated quarantine multiple times without having even stepped outside their houses once. The Corona Mukt Himachal application, for example, has incorrectly recorded violations of quarantine which has further led to police complaints being filed against individuals.[52]

# 5. Conclusion

This report alongside its tracker intends to capture and analyse emergent tech tools being used to contain the effects of the pandem. In response to Covid-19, numerous studies have surfaced focusing on the more apparent issues of data protection and privacy, dwelling less on the broader systemic changes occurring as society adapts to the pandemic. The report therefore attempts to bring these broader considerations to the fore, providing a glimpse into how the digital health ecosystem is evolving,and related levels of institutional and regulatory readiness..

Through the review of these tools, we raise important questions around the risks of technological and societal lock-ins. In order to gauge these various concerns that emerge, we utilised this report as a way to iteratively develop a framework for responsible tech adoption.

We highlight a few key takeaways as part of this conclusion to emphasise that most of the tools do not stand the test of the parameters in place. Even while some good apples appear fruitful, they do not function without significant risks.

- The technological response only further demonstrates the increasingly dire need for a contextually situated responsible tech framework.

- Many of the tools fail to be inclusive and equitable in not only their functionality but also in their deployment. For example, a large number are not available for use on feature phones or in regional languages.

- Privacy and data protection continue to be major concerns despite the growing awareness around their need, as very few tools have data protection policies in place.

- Most tools have no forms of accountability mechanisms or grievance redressal systems. As these are tools developed to aid the public health care space, it is crucial that they must embody values of trust and reliability.

- There is a serious legal and policy vacuum around the regulation of rapidly developing technologies which is imperative to encourage the development of safe technological systems.

- There is also a glaring gap in publicly available information on the measures that assess the scientific validity and general efficacy of these technological solutions to a global pandemic. There is a need for the establishment of robust verification and evaluation systems.

# 6. References

1. Aarogya Setu Privacy Woes: Over 40 Organisations Push Back Against Mandatory Usage of Covid-19 App. (2020, May 03). Retrieved from https://thewire.in/rights/aarogya-setu-privacy-woes-letter

2. Koops, B. J., Oosterlaken, I., Romijn, H., Swierstra, T., & Van den Hoven, J. (Eds.). (2015). Responsible innovation 2: concepts, approaches, and applications. Springer.

3. Von Schomberg, R. (2011). Towards responsible research and innovation in the information and communication technologies and security technologies fields. Available at SSRN 2436399.

4. Stahl, B. C., Eden, G., & Jirotka, M. (2013). Responsible research and innovation in information and communication technology: Identifying and engaging with the ethical implications of ICTs. Responsible innovation, 199-218.

5. Shunmugasundaram, M. (2020, May 08). India needs to enact a COVID-19 law. Retrieved from:https://www.thehindu.com/opinion/lead/india-needs-to-enact-a-Covid-19-law/article31529036.ece

6. Pandey, G. (2020). Coronavirus in India: Desperate migrant workers trapped in lockdown. BBC News. https://www.bbc.com/news/world-asia-india-52360757

7. Singh, V. (2020). India's Aarogya Setu Contact Tracing App: Compromising privacy in a pandemic. Jurist. https://www.jurist.org/commentary/2020/05/vidisha-singh-aarogya-setu-app-Covid19/

8. DISHA and the draft Personal Data Protection Bill, 2018: Looking at the future of governance of health data in India. (2019). Ikigai Law. https://www.ikigailaw.com/disha-and-the-draft-personal-data-protection-bill-2018-looking-at-the-future-of-governance-of-health-data-in-india/

9. Sharon, T. Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. Philos. Technol. 30, 93–121 (2017). https://doi.org/10.1007/s13347-016-0215-5

10. Silva, H. P., Lehoux, P., Miller, F. A., & Denis, J. L. (2018). Introducing responsible innovation in health: a policy-oriented framework. Health research policy and systems, 16(1), 90.

11. Claburn, T. (2020, May 21). Apple, Google begin to spread pro-privacy, batt-friendly coronavirus contact-tracing API for phone apps. Retrieved from https://www.theregister.com/2020/05/21/apple_google_coronavirus_api/

12. Sircar, S. (2020, April 16). Covid-19: What Happens to RTIs During the Lockdown? Retrieved from https://www.thequint.com/news/india/Covid-19-coronavirus-what-happens-to-rti-during-lockdown

13. MoHFW. (2020, March 25). Telemedicine Practice Guidelines. Retrieved from https://www.mohfw.gov.in/pdf/Telemedicine.pdf

14. 500% rise in healthcare teleconsultation in India, 80% are first-time users: Report. (2020, June 30). Retrieved from https://indianexpress.com/article/lifestyle/health/500-increase-in-healthcare-teleconsultation-in-india-80-are-first-time-users-report-6483212/

15. Telemedicine, Preventive Healthcare To Shape India's Healthtech Landscape In Post-Covid World. (2020, July 01). Retrieved from https://inc42.com/datalab/telemedicine-preventive-healthcare-to-shape-indias-healthtech-landscape-in-post-Covid-world/

16. See, https://www.docsapp.in/

17. DocsApp & PhonePe come together to enable online doctor consultations. (2020, April 30). Retrieved from https://www.expresscomputer.in/news/docsapp-phonepe-come-together-to-enable-online-doctor-consultations/54462/

18. 500% rise in healthcare teleconsultation in India, 80% are first-time users: Report. (2020, June 30). Retrieved from https://indianexpress.com/article/lifestyle/health/500-increase-in-healthcare-teleconsultation-in-india-80-are-first-time-users-report-6483212/

19. Snapchat rolls out 'Here for You' feature in India to help users tackle mental health problems; Details. (2020, July 14). Retrieved from https://www.financialexpress.com/industry/technology/snapchat-rolls-out-here-for-you-feature-in-india-to-help-users-tackle-mental-health-problems-details/2023578/

20. Indo-Asian News Service. (2020, January 30). Over 500 Million Indians Now Use Smartphones, Report Claims. Retrieved from https://gadgets.ndtv.com/mobiles/news/over-500-million-indians-now-use-smartphones-77-percent-of-who-are-online-techarc-2172219

21. Tripathi, S., Jain, N., Kumar, A., Sanghi, K., Bansal, A., & Bajaj, S. (2017, June 21). Encashing on Digital: Financial Services in 2020. Retrieved from https://www.bcg.com/en-in/encashing-on-digital-financial-services-in-2020

22. Kapoor, M., Agrawal, D., Ravi, S., Roy, A., Subramanian, S., & Guleria, R. (2019, August 08). Missing women patients: Gender discrimination in access to healthcare. Retrieved from https://www.brookings.edu/blog/up-front/2019/08/08/missing-women-patients-gender-discrimination-in-access-to-healthcare/

23. DocsApp Patients Can Talk to Doctors in 17 languages, including Hindi and English. (2017, December 28). Retrieved from https://indiamedtoday.com/docsapp-patients-can-talk-to-doctors-in-17-languages-including-hindi-and-english/

24. See, https://www.wysa.io/media. Wysa has about 8 languages translated by volunteers, however, there are no reports to confirm the rolling out of the application in various languages.

25. See, https://Covid19jagratha.kerala.nic.in/

26. We are assuming this clause to be applicable to the Covid-19 risk assessment tool rolled out by DocsApp as well.

27. Sriram, J. (2016, September 22). Taking eye care to every corner of rural India. Retrieved from https://www.thehindu.com/news/cities/mumbai/business/Taking-eye-care-to-every-corner-of-rural-India/article13980789.ece

28. Chellaiyan, V. G., Nirupama, A. Y., & Taneja, N. (2019). Telemedicine in India: Where do we stand? Journal of Family Medicine and Primary Care, 8(6), 1872. doi:10.4103/jfmpc.jfmpc_264_19

29. Kapoor, A. (2020, July 28). Pulse oximeter: Monitor your pulse rate and blood oxygen levels accurately - Times of India. Retrieved from https://timesofindia.indiatimes.com/most-searched-products/health-and-fitness/health-care/pulse-oximeter-monitor-your-pulse-rate-and-blood-oxygen-levels-accurately/articleshow/71817417.cms

30. IANS. (2019, August 22). Hackers attack Indian healthcare website, steal 68 lakh records - ET CISO. Retrieved from https://ciso.economictimes.indiatimes.com/news/hackers-attack-indian-healthcare-website-steal-68-lakh-records/70782910

31. Loaded with new tech 'Indore 311' mobile app to track, tackle asymptomatic COVID-19 patients - ET Government. (2020, May 08). Retrieved from https://government.economictimes.indiatimes.com/news/digital-india/loaded-with-new-tech-indore-311-mobile-app-to-track-tackle-asymptomatic-Covid-19-patients/75608383

32. Chellaiyan, V. G., Nirupama, A. Y., & Taneja, N. (2019). Telemedicine in India: Where do we stand? Journal of Family Medicine and Primary Care, 8(6), 1872. doi:10.4103/jfmpc.jfmpc_264_19

33. RK Dewan & Co. (2020, May 13). Personal Data Protection Laws in India. Retrieved from https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d

34. Rule 4 of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

35. Monahan, T., & Wall, T. (2002). Somatic Surveillance: Corporeal Control through Information Networks. Surveillance & Society, 4(3). doi:10.24908/ss.v4i3.3446

36. Sirur, S. (2020, August 01). How India increased its Covid testing capacity from 52 labs to over 1,300 in 4 months. Retrieved from https://theprint.in/health/how-india-increased-its-covid-testing-capacity-from-52-labs-to-over-1300-in-4-months/471262/

37. As of June 2018, TOI reported that India has only 960 testing labs across the country, of which 703 are government accredited and 257 are private. TNN. (2020, July 04). Why Covid testing is a slow process and types of tests available - Times of India. Retrieved from https://timesofindia.indiatimes.com/india/why-Covid-testing-is-a-slow-process-and-types-of-tests-available/articleshow/76459365.cms

38. Mobile detection stations for collection of swabs. (2020, April 08). Retrieved from https://www.thehindu.com/news/cities/Hyderabad/mobile-detection-stations-for-collection-of-swabs/article31292736.ece

39. COVID-19 Contact Tracing. (2020, August 04). Retrieved from https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html

40. Exit through the App Store? (Rep.). (2020, April 20). Retrieved https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf

41. Digital India: Technology to Transform a Connected Nation. McKinsey Global Institute. (March 2019)

42. State wise quarantine regulation -Customer Support Guide Version-13. IndiGo. Retrieved from https://www.goindigo.in/content/dam/indigov2/6e-website/banners/2020/State-wise-quarantine-regulation-v13.pdf

43. M, A. (2020, July 11). Surge in cases puts contact-tracing off track in Karnataka. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/surge-in-cases-puts-contact-tracing-off-track-in-karnataka/articleshow/76904989.cms

44. PTI. (2020, May 08). Aarogya Setu most downloaded healthcare app in world: Amitabh Kant. Retrieved from https://economictimes.indiatimes.com/tech/internet/aarogya-setu-most-downloaded-healthcare-app-in-world-amitabh-kant/articleshow/75633564.cms

45. Agrawal, A. (2020, July 10). Petitioner to amend PIL against mandatory use of Aarogya Setu in Karnataka HC. Retrieved from https://www.medianama.com/2020/07/223-aarogya-setu-pil-karnataka-hc-amendment/

46. Agrawal, A. (2020, July 27). Aarogya Setu mandatory to enter Saket Court Complex in Delhi. Retrieved from https://www.medianama.com/2020/07/223-aarogya-setu-mandatory-saket-court/

47. Dixit, P. (2020, May 01). For A Billion Indians, The Government's Voluntary Contact Tracing App Might Actually Be Mandatory. Retrieved from https://www.buzzfeednews.com/article/pranavdixit/for-a-billion-indians-the-governments-voluntary-contact

48. Butani, A. (2020, May 06). No Aarogya Setu app? Pay Rs 1,000 fine or face 6 months jail in Noida. Retrieved from https://indianexpress.com/article/cities/delhi/aarogya-setu-app-fine-jail-noida-6394954/

49. Bilinski, A., Mostashari, F., & Salomon, J. A. (2020). Contact tracing strategies for Covid-19 containment with attenuated physical distancing. medRxiv.

50. Mehrotra, K. (2020, April 11). Behind Aarogya Setu app push: 'At least 50% people must download for impact'. Retrieved from https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/

51. Rule 4 of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

52. Puri, S. (2020, May 09). HP Covid app defective, people facing legal actions complain: Shimla News - Times of India. Retrieved July 31, 2020, from https://timesofindia.indiatimes.com/city/shimla/hp-Covid-app-defective-people-facing-legal-actions-complain/articleshow/75641704.cms