

Privacy prescriptions for technology interventions on Covid-19 in India

by

*Sidharth Deb,
Policy and Parliamentary Counsel,
Internet Freedom Foundation
sidharth@internetfreedom.in*

Abstract

With a view to address the public health challenges due to the highly infectious nature of Covid-19 a range technology interventions are being developed that impact personal privacy. The objective of this working paper is to inform public policy formation in India across various stakeholders specifically government authorities, technologists, public health practitioners and digital rights groups. To achieve this the working paper first aims to comprehensively document these developments and also adopt a comparative review of international literature. This includes a substantive analysis of the use and publication of health data, specific development of surveillance technologies around location tracking and finally the deployment of contact tracing through handheld device applications. We devote substantial space to a front-end analysis of three contact applications Singapore's TraceTogether, MIT's Private Kit : Safe Path's Project and Aarogya Setu. We also consider the possible public policy and rights related ramifications of the recent announcement of a partnership between Apple and Google towards contact tracing. To conclude we make substantial prescriptions premised primarily on the legal framework of the Indian Supreme Court's developing jurisprudence on the fundamental right to privacy as reaffirmed in Hon'ble Supreme Court's judgement in *KS Puttaswamy (Retd) and Anr v Union of India* [(2017) 10 SCC 1.

Cite as: Deb, Sidharth, Public Policy Imperatives for contact tracing in India (April 11, 2020). IFF Working Paper No. 3/2020. Available at SSRN: [\[awaits approval\]](#)

Acknowledgments: The author would like to thank Aravind RS, Karthik B. and Raman C. trustees at the Internet Freedom Foundation for initial analysis. Further suggestions and review was received from IFF staff including Devdutta M. and Apar G.

Request for open collaboration: This working paper has been authored at pace and is a work in progress. It aims to match the continued development of technology interventions that offer great promise and can integrate functional design values aligned with the fundamental right to privacy in India. This can only be achieved with open collaboration, comment and review. To aid this the working paper is being made publicly accessible as a google document. Also, you may further provide inputs (with or without attribution) on the [Internet Freedom Forum](#) or by sending an email to policy@internetfreedom.in. A google docs copy of this paper is available here for the convenience of comment and making suggestions.

1. Public health strategies around Covid-19	3
2. Tech deployments & privacy imperatives	6
The puttaswamy-privacy framework	6
International human rights standards	8
3. Collection, use and dissemination of personal health records & related information	9
Collection, user and disclosure of health data	9
Illegality of unauthorised disclosures	10
4. Location tracking and electronic fencing	11
Use case for location tracking	11
India's deployment of location tracking	11
International practices on location tracking	13
Case study 1: Europe	14
Case study 2: Asia	16
Case study 3: Israel	18
Case study 4: United State of America	20
Government	20
Non-government	22
Limitations in location tracking	24
How can governments allay your fears?	25
5. Contact tracing apps, websites and platforms	26
Future of technology for disease control?	26
International development of contact tracing apps	28
Case Study 1: Singapore	28
Case Study 2: Asia	30
Case Study 3: Europe	32
Pan-European Privacy-Preserving Proximity Tracing Project	33
Views of regional European authorities	35
Case Study 4: Latin american approaches	35
Surveillance firms eye profit & reputational laundering	36
Development of contact tracing interventions in India	37
Committee for developing a citizen app technology platform	37
Prior projects by the Government of India	38
Panoply of state government apps	40
Preventing mass surveillance through contact tracing	42
Assessing need, feasibility and risks	42
Promising models for contact tracing applications	43
Design and rights imperatives for contact tracing applications	45
6. Incentive structures for adoption	47
Sensitivity to individual autonomy furthers user trust	48
Case study: Iran	49
7. Analysis of contact tracing applications developed by Singapore, MIT and India	50
Case study 1: TraceTogether (Singapore)	51
Permissions sought : user consent is present but not absolute	52

Privacy and security safeguards : do users have full control?	53
State-coercion to access contact tracing information	54
So how do users audit these representations?	55
<i>Case Study 2: PrivateKit : SafePaths (MIT)</i>	55
Underlying principles and assumptions of the project	55
Design features : towards a privacy-first app	56
Specifics of the application and its privacy practices	57
Auditability of the application	59
<i>Case study 3: Aarogya Setu (Government of India)</i>	59
Background to the application	59
A systemic lack of auditability and transparency	60
Uncoding the underlying assumptions of Aarogya Setu	61
Frontend Analysis through the Terms of Service & Privacy Policy	62
Terms of Service (TOS) of Aarogya Setu	63
Broad permissions and data maximisation	63
Severe restrictions undermine trust	64
Vague frameworks for discretionary action without objective standards	65
Privacy Policy of Aarogya Setu	65
Ideal standards of a Privacy Policy	65
Information collected adopts an approach towards data maximisation	66
Information exchange and storage opens up multiple threat vectors	67
Purpose limitation is undercut by its exceptions	67
Data Retention for now and forever?	69
User Rights exist to seek deletion. That's it.	69
Data Security Safeguards exist but remain unverifiable.	69
Establishes a system for remedy by provisioning for a Grievance Officer	70
Vagueness on data transfers	70
Urgent need for transparency and clear limits	70
Imperatives for Rule of Law Compliant Contact Tracing	72
Recommendations	73
8. A partnership of (silicon valley) giants	77
Background of the Apple and Google partnership	77
The announcement	77
Technical features of the partnership project	78
Sequencing of the project	79
Unique risks due to private sector initiative	80
Enhanced need for checks and balances	80
Negotiating government use of personal data	81
Issues of Competition and conflicts of interest	82
Should such projects be controlled by trans-national corporate entities?	82
Conclusion and final recommendations	85

1. Public health strategies around Covid-19

1. As India considers response strategies to the novel SARS-COV2 disease which is known more commonly as COVID-19, the country is encountering a seemingly hobbesian trap. It is currently in the middle of a country-wide lockdown which is globally unprecedented in terms of scale. Decision makers hope that radical, preventive actions will be instrumental in slowing the rate of person-to-person transmission and afford sufficient space to ratchet up healthcare capacity.
2. The lockdown has also precipitated a multitude of humanitarian and economic challenges. First, despite a complete shutdown of transportation systems we saw a mass exodus of immigrants from urban to rural areas. Many of these people sought to return to their homes on foot-- sometimes willing to walk hundreds of kilometres. Second, there has been a disruption of supply chains-- harming last mile delivery of crucial items. As is the case with the rest of the world, the lockdown also means public consumption is shrinking fast and the economy is invariably slowing down. The ramifications of this are being felt by large segments of the people, especially those working in the informal sector.
3. Any decision to prolong the lockdown (to ride out the effects of the novel virus) is riddled with complex economic and human security risks. The reality is that the virus will not be eradicated by April 14, 2020. Epidemic models predict that infections will rise rapidly when the lockdown ends¹, and it can only be mitigated through swift and decisive action. The risks with the disease and the need for expedited action are magnified since there is no available vaccine. Many experts suggest that it is unlikely that a reliable vaccine will be available in the market for the next 18 months.² Even after it comes to the market, it is likely to take several months before production capacity is large enough to meet global demands.
4. Therefore, the entire world including India, stares at a significant period of unprecedented uncertainty. There is also a looming threat of economic collapse which may inflict significant portions of India's 1.3 billion plus population. India is also disadvantaged due to a large segment of population being close to the poverty line and must make hard choices with respect to allocation of scarce capacity. To navigate this, it is incumbent for the Indian Government to deploy best in class practices to solve challenges in an agile manner.

¹ Rajesh Singh and R. Adhikari, *Age-structured impact of social distancing on the COVID-19 epidemic in India*, March 2020, <https://arxiv.org/pdf/2003.12055.pdf>.

² Rob Grenfell and Trevor Drew, *Here's Why it Takes So to Develop a Vaccine for the New Coronavirus*, Science Alert, February 2020, <https://www.sciencealert.com/who-says-a-coronavirus-vaccine-is-18-months-away>.

5. Here, it is prudent to follow recommendations of doctors and epidemiologists i.e. practitioners who study the spread of disease. International organisations like the World Health Organisation (WHO) have articulated four key pillars as the 'backbone' of effective response strategies; namely *testing, isolation, tracing and treatment*.³ The following is how this paper interprets these four pillars:
 - A. Testing: While being mindful of resource constraints, India must ratchet up its testing infrastructures and capacity. Testing helps in early detection and containment, in terms of pace and spread of disease.
 - B. Isolation/Quarantine: Moving forward, isolation must be nuanced and localised. It must preserve economic activity, minimise discriminatory outcomes, preserve individual agency, protect minorities and minimise privacy harms. Isolation and/or lockdowns should not be done arbitrarily but rather based on reliable evidence/data which is publicly available. A related element which is key to response strategies is effective tracing.
 - C. Tracing: Most health experts and epidemiologists emphasise the importance of contact tracing in containing the speed of spread. However, the difficulty arises in terms of modalities. For effective contact tracing we need to engender trust. It must be agile, human centric and rights respecting. Frameworks for contact tracing must be aligned with constitutional thresholds on restrictions to the right to informational privacy. Moreover, these frameworks must be sustainable and evidence based. Conversely, they should not stoke fear or panic among communities.
 - D. Treatment: Treatment strategies should be informed by the views of healthcare experts. The government must allocate sufficient resources and simultaneously steer investments towards testing, beds, ventilators, medication and Personal Protective Equipment (PPEs) for the safety of healthcare providers.

As mentioned earlier, we are racing against time and working with limited resources. Hence, strategic deployment becomes a key public policy priority.

2. Tech deployments & privacy imperatives

1. A key way to maximise efficiency is contact tracing. It is articulated as having the potential to proactively identify hotspots and can allow for swift localised

³ Linda Lacina, WHO coronavirus briefing: Isolation, testing and tracing comprise the 'backbone' of response, World Economic Forum, March 2020, <https://www.weforum.org/agenda/2020/03/testing-tracing-backbone-who-coronavirus-wednesday-briefing/>; Also See WHO's T3 Initiative i.e. T3: Test. Treat. Track. Initiative for Malaria, https://www.who.int/malaria/areas/test_treat_track/en/

decision making, without stressing resources more than the strict necessary minimum. According to a recent report by Access Now⁴, public authorities are trying to leverage technological solutions in tracing novel coronavirus in the following ways:

- A. Collection, use and dissemination of people's personal health records and related information;
 - B. Tracking of location data; and
 - C. Public-private partnerships towards building apps, websites and platforms to combat COVID-19.
2. As India's brush with the novel virus has accelerated, the response tactics are also evolving. To this end, the Indian Government is placing considerable bets on the use of surveillance toward containment efforts. For instance, the country's senior most bureaucrat i.e. the Cabinet Secretary, Mr Rajiv Gauba reportedly wrote to state governments to maintain stringent surveillance protocols to track around 1.5 million people with international travel histories.⁵

The puttaswamy-privacy framework

3. Here, it becomes important to highlight the Hon'ble Supreme Court's judgement in *KS Puttaswamy (Retd) and Anr v Union of India* [(2017) 10 SCC 1]. In it the Court recognised the right to privacy as a part of the right to life and personal liberty protected under Article 21 of India's Constitution. Within it, the Hon'ble Supreme Court observed that:

"An unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy. On the other hand, the state may assert a legitimate interest in analysing data borne from hospital records to understand and deal with a public health epidemic... to obviate a serious impact on the population. If the State preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions."

4. The Supreme Court also cites several cases discussing how an invasion into people's privacy vis-a-vis health records can have deleterious effects on a person's standing in society, and lead to tremendous discriminatory outcomes.

⁴ Recommendations on Privacy and Data Protection in the Fight Against COVID-19, Access Now, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>

⁵ 'There is a gap': Cabinet Secretary raises red flag on COVID-19 surveillance, Hindustan Times, March 2020, <https://www.hindustantimes.com/india-news/may-jeopardise-efforts-cabinet-secretary-redflags-gap-in-covid-19-surveillance/story-sXQ5TFwB5QKuQrGbF2etIJ.html>.

Admittedly, the Court observes that the right to privacy as is the case with the right to life is not absolute. However, any curtailment or deprivation must take place under a regime of law. Therefore, any restriction on the right must satisfy four discrete requirements. They include⁶:

- A. Legality: i.e. there must be a clear law and provision;
 - B. Necessity and purpose: must have a legitimate aim/purpose and must be necessary in a democratic society i.e. in the interests of national security, public safety, for the prevention of disorder and crime, or for the protection of health or morals;
 - C. Proportionality: must be proportionate where the measure has a rational nexus with the legitimate aim sought to be achieved; and
 - D. Safeguards: have in-built procedural safeguards aligned with standards of procedure established by law which are just, fair and reasonable to prevent abuse.
5. In other words the state measure must satisfy requirements of necessity and proportionality. The chosen measure must be the least restrictive of all means available to achieve the objective. Moreover, when it comes to interpreting “legitimate purpose”, there is presumption that the purpose is singular and precise. If the data of an individual is collected for one purpose and it is used subsequently for a different purpose without the informed consent of the individual it would amount to a violation of the right to privacy. Moreover, any mechanism for consent for general purpose data sharing conflicts with this strict purpose limitation principle.

International human rights standards

6. Given the seriousness of the virus which has been classified as a pandemic⁷, this paper utilises the thought and recommendations of international organisations and experts and then situate them in India. We have drawn guidance from organisations and institutions like Access Now, Electronic Frontier Foundation, Fraunhofer Institute for Telecommunications, Massachusetts Institute of Technology, Pan-European Privacy Preserving Proximity Tracing Project, Privacy International and others. We also make extensive reference to commentary by

⁶ Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. *IndraStra Global*, 11, 1-5. <https://nbn-resolving.org/urn:nbn:de:0168-ssaoar-54766-2>.

⁷ Dr Tedros Adhanom Ghebreyesus, *WHO Director General's Opening Remarks at the Media Briefing on COVID-19*, 11 March 2020; World Health Organisation, <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>.

Adam Schwartz, Professor Hu Yong, Ryan Calo, Sean McDonald, Shoshana Zuboff, Susan Landau, Yves-Alexandre de Montjoye, Florimond Houssiau, Andrea Gadotti, Florent Guepin and many others.

7. While we may specifically refer to their analysis, there exists broad consensus that in times of a health crisis, policymakers may introduce extraordinary measures which must comply with human rights and constitutional standards. Such extraordinary measures allow states to derogate from maintaining people's fundamental freedoms⁸ provided they are done so: (i) under exceptional circumstances, (ii) in a limited capacity and (iii) in a supervised manner.⁹
8. Nonetheless, any special legal order to derogate people's fundamental freedoms including the right to privacy is subject to the rule of law. Measures thereunder cannot subsist for an indefinite period and must have a defined sunset clause.¹⁰ Considerations of proportionality include severity of the restriction itself, duration of the restriction (temporal) and geographical reach. It must also be ensured that the restriction actually helps in mitigating risks pertaining to the crisis. Anything beyond this would be incompatible with the rule of law.
9. This is important to impress since these are the necessary legal and institutional requirements to legitimise any intrusion into people's informational privacy. Therefore, state action to trace, detect and contain the spread of COVID-19 must necessarily conform with these thresholds.

3. Collection, use and dissemination of personal health records & related information

1. Since the third week of March India has witnessed the indiscriminate sharing of lists of persons who are suffering from Covid-19 infection; or, are suspected of being carriers; or, fall within a risk category due to recent travel. These lists of persons are being principally shared through digital means. This increases the

⁸ Certain rights do not allow for derogation, like the right to life, the prohibition of torture and inhuman or degrading treatment or punishment, the prohibition of slavery, and the rule of "no punishment without law." (As articulated by Access Now in <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>).

⁹ Read Generally: Recommendations on Privacy and Data Protection in the Fight Against COVID-19, Access Now, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>.

¹⁰ Hungarian Civil Liberties Union. Unlimited power is not the panacea, 2020. <https://hclu.hu/en/articles/unlimited-power-is-not-the-panacea>; as cited in Recommendations on Privacy and Data Protection in the Fight Against COVID-19, Access Now, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>.

field of dissemination of personally identifiable information and can lead to acute harm.

Collection, user and disclosure of health data

2. We have already observed certain damaging, irresponsible and illegal responses by state-level Indian authorities on this front. Specifically, they are rather comfortably disclosing to the public details like the name, home & address, travel history, etc. of people who have been put under quarantine. Multiple state governments (across party lines) have been seen to engage in such practices including Karnataka¹¹ and Punjab.
3. The Internet Freedom Foundation (IFF) filed a representation with multiple authorities including the Ministry of Health and Family Welfare; and the Ministry of Housing and Urban Affairs, on the illegality of such quarantine lists. IFF represented that they lead to discrimination, social ostracisation, denial of access to essential items, eviction from rented accommodations and have harmful impacts on the concerned person and their friends and family.¹²
4. Authorities have also used indelible ink to stamp people who have been ordered to quarantine themselves.¹³ Similarly, we have seen authorities in places like Delhi and Punjab where authorities are physically marking homes in which the inhabitants have been ordered to self-quarantine.¹⁴
5. To draw an analogy, the use of such tactics to leverage the power of social coercion can lead to ostracisation which is reminiscent of the conditions people faced when it was disclosed to the public and communities they may have contracted the HIV virus or Tuberculosis. Moreover, it is in direct opposition to the Supreme Court's mandate in the right to privacy judgement.

¹¹ Naveen Menezes and Bellie Thomas, *Government Publishes Details of 19,240 home quarantined people to keep a check*, Bangalore Mirror, March 2020, <https://bangaloremirror.indiatimes.com/bangalore/others/government-publishes-details-of-19-240-home-quarantined-people-to-keep-a-check/articleshow/74807807.cms>

¹² *Quarantine lists breach individual privacy! Social solidarity in times of Covid-19 #SaveOurPrivacy*, Internet Freedom Foundation, March 2020, <https://internetfreedom.in/quarantine-list/>

¹³ *Election Commission allows the use of indelible ink for stamping 'home quarantined'*, Economic times, March 2020, <https://economictimes.indiatimes.com/news/politics-and-nation/election-commission-allows-use-of-indelible-ink-for-stamping-home-quarantined/articleshow/74820647.cms>

¹⁴ Angana Chakrabarti, *Delhi govt marks homes under COVID-19 quarantine – 4 times world saw such isolations before*, The Print, March 2020, <https://theprint.in/health/delhi-govt-marks-homes-under-covid-19-quarantine-4-times-world-saw-such-isolations-before/385900/>

Illegality of unauthorised disclosures

6. In times of a public health crisis¹⁵ that it is key to ascertain *how a government can access and use health data to fight public health crises*. Unfortunately, India is in a disadvantaged position since it lacks a comprehensive personal data protection framework. Existing legal provisions have extremely limited efficacy. For instance Section 43A of the Information Technology Act (IT Act), 2000; and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules (“SPDI Rules”), 2011 have limited applicability and suffer from a lack of enforcement.
7. To its credit, Rule 3(iii) of the SPDI Rules includes “*physical, physiological and mental health condition*”(s) under the category of sensitive personal data or information. Moreover, both the 2018 and 2019 drafts of India’s Personal Data Protection Bill, have included health data as falling under sensitive personal data. In an ideal world users should have greater control over any access or use of sensitive personal data. Unfortunately, without a comprehensive data protection law there is no privacy-respecting pathway for the regulated use of health data by public authorities and private parties.
8. Authorities would still be required to comply with the Hon’ble Supreme Court’s judgement in *KS Puttaswamy v Union of India* [(2017) 10 SCC 1]. In it the Court explicitly observes that when it comes to a public health epidemic, authorities may use health records, provided they ensure the anonymity of the patients. Nevertheless, public authorities do not have a stable framework through which they can reliably use public health information to mitigate the spread of the virus in a manner consistent with requirements of necessity, proportionality and purpose limitation.

4. Location tracking and electronic fencing

1. While the disclosure of personal information by, “lists’ ” was the first wave of technology implementation it is becoming more sophisticated. Even as India struggles with availability of physical and human resources, we are seeing attempts to leverage modern technologies to support these activities. One such avenue has been governments using technology as a trigger to coerce desirable human responses. Monitoring of people’s location through mobile devices has been repeatedly brought up as a means towards. However, the use of such options is fraught with human-side risks.

¹⁵ Recommendations on Privacy and Data Protection in the Fight Against COVID-19, Access Now, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>

Use case for location tracking

2. On March 26 2020, Michael Ryan, Executive Director of the WHO, stated that collecting people's personal information or their whereabouts/movements brings with it serious implications for data protection.¹⁶ After all, location data can be very revealing. Parties with access to such data may deduce your home and work address, your socioeconomic status, aspects relating to identity (like religion or caste), and can reveal much more.
3. From the perspective of disease control, it is important to consider that the location of people's smartphones in isolation is not useful in tracking the spread and evolution of the virus. It is only when such information is combined with information on persons infected with the virus, is when location data can support risk mitigation responses. Both domestically and internationally authorities are nevertheless, mobilising existing (sometimes archaic) national security and interception frameworks to access these people's location coordinates-- through cell towers and/or GPS coordinates.

India's deployment of location tracking

4. To the best of our knowledge, the most prominent instance of location tracking via cell phones in India is administered by the State of Delhi. Delhi's Chief Minister, Arvind Kejriwal disclosed a programme where the state is administering individualised location tracking. This is being done to assess if people who have been officially ordered to quarantine themselves are adhering to government directives. He revealed that the names of 25,429 individuals had been shared with the Delhi Police. These lists are shared by the Chief Minister in consultation with the Lieutenant Governor of Delhi.
5. Civil society organisations like IFF have previously expressed concern that there was no mention of the legal framework under which this was being administered. Moreover, in the absence of a legal order there is no way to confirm if enforcement authorities have any limitations in terms of access and use of people's personal data. Therefore, IFF has clearly stated that this initiative appears incompatible with the rule of law, which remains a prerequisite even in times of a public health crisis.¹⁷ This is not the only example of the use of surveillance technologies in Delhi. For example, the Delhi Police reportedly

¹⁶ World Health Organisation. COVID-19 virtual press conference - 25 March 2020. <https://www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-pressconference-full-25mar2020.pdf>

¹⁷ Statement by Internet Freedom Foundation on Delhi Chief Minister's Announcement on Location Surveillance of Quarantined Individuals, Twitter, April 2020, <https://twitter.com/internetfreedom/status/1245364494705897473>

accessed drone footage in Delhi's Nizamuddin West area, to review video feeds of people's involvement in a large religious gathering which became a hotspot and exaggerated the spread of the virus in India.¹⁸

6. Other states in India are also deploying a combination of location surveillance and other technologies to ensure people comply with quarantine/isolation requirements. In Kerala authorities have reportedly used a combination of call records, phone location data and surveillance camera footage to check if people have been in contact with infected persons.¹⁹
7. In Tamil Nadu, police in the Tiruvallur district are using an Android application called CoBuddy which deploys facial recognition along with geofencing to keep track of people under quarantine. People must provide the app access to their GPS location and a picture of their face. Police receive prompts should the individual move outside the geofence which can be set 10 metres to 100 metres outside the individual's home. Additionally, to ensure they do not leave their phone the app requests people to share a photo of their face 2-3 times (at random) with the app, which is verified against the original photo. Although it is not verifiable (and there is no trace of a privacy policy), it must be stated that the app's developer claims that the app does not store any personal data including uploaded photos. They assert that the police are provided access to a user's GPS coordinates and the individual's unique identifier.
8. Another prominent instance of state level adoption of technology to control people's movement is the Karnataka Government's Android app called *Quarantine Watch*. People under quarantine in Karnataka are required to download the application and share hourly photos (between 7:00 AM and 10:00 PM) in conjunction with GPS location coordinates. Should people fail to abide by the hourly requirements, a Government response is expected to reach the homes of the concerned person under quarantine. Each of these photos is geo-tagged and is verified by a Government photo-verification team. If an individual sends a wrong photo, a person runs the risk of being transferred to a mass quarantine centre.²⁰

¹⁸ Vasudha Venugopal, Aarogya Setu, drone data to play part in lockdown exit strategy, Economic Times, April 2020, <https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/aarogya-setu-drone-data-to-play-part-in-lockdown-exit-strategy/articleshow/75040648.cms?from=mdr>

¹⁹ Arjun Kharpal, Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends, CNBC, March 2020, <https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html>

²⁰ COVID-19 | People in home quarantine told to send selfies every hour to govt, The Hindu, March 2020, <https://www.thehindu.com/news/national/karnataka/covid-19-people-in-home-quarantine-to-ld-to-send-selfies-every-hour-to-govt/article31208001.ece>

International practices on location tracking

9. Location tracking practices are not novel to India. In the face of the novel coronavirus several countries are adopting such measures to track people's location/movements for disparate purposes. The purposes for such deployment may be epidemiological in nature (in identifying spread and potential hotspots), to notify individuals of potential risk of infection, to measure social distancing and occasionally governments use these technologies to ensure compliance with isolation/quarantine orders, curfew measures and to measure social distancing.
10. For instance, Kenya²¹ and Ecuador²² are deploying "electronic surveillance" to track individuals who have been ordered to self-isolate. This is done by monitoring mobile activities including location data. Governments in these countries have ordered citizens to not switch off their mobile devices and to keep them on their persons. In South Africa, TSPs are entering into extra legal arrangements with its nodal telecom and communications authorities to share data analytics with respect to people's location. What is notable is that the telecom authorities forward these datasets to other government agencies as well. It remains unclear whether the arrangement only pertains to the personal data of infected persons or people from across the country.²³

Case study 1: Europe

11. Such backchanneling/extra-legal arrangements between government authorities and TSPs appears to be common in Europe as well. For instance, Belgian²⁴ telecom operators are granting public authorities access to "parts" of their databases. Similarly, in Germany Deutsche Telekom is affording its Federal

²¹ The Standard Media. State Taps Phones of Isolated Cases, 2020.

<https://www.standardmedia.co.ke/article/2001365401/state-taps-phones-of-isolated-cases>

²² As cited in *Recommendations on Privacy and Data Protection in the Fight Against COVID-19*, Access Now, March 2020,

<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>

²³ Business Insider SA. South Africa will be Tracking Cellphones to Fight the Covid-19 Virus. 2020,

<https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3>

²⁴ As cited in *Recommendations on Privacy and Data Protection in the Fight Against COVID-19*, Access Now, March 2020,

<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>; Le Soir. Coronavirus: le cabinet De Block dit «oui»

à l'utilisation des données télécoms, 2020. <https://plus.lesoir.be/286535/article/2020-03-12/coronavirus-le-cabinet-de-block-dit-oui-l-utilisation-des-donnees-telecoms>.

Disease Prevention Agency “partial” access to its location data to help contain the pandemic.

12. More specifically, media reports indicated that telecom service providers²⁵ in Germany, Italy and Austria respectively, were sharing data with national health authorities. The data is structured to be aggregated and anonymised and can inform authorities about concentrations, movements and hotspots of gathering²⁶. In Austria, data shared by TSPs with health authorities includes insights gleaned from a motion analysis app.²⁷ An anomalous aspect of the Italian approach is that unlike other European states, in Lombardy, authorities are reportedly using location data to gauge compliance with lockdown orders.²⁸
13. At a regional level, the European Commission²⁹ has reached out to telecom majors in the region to share people’s mobile data to help “*predict the spread of the virus*”. Specifically, they have requested the operators to share anonymised and aggregated data from mobile devices to understand how the disease itself was spreading. What is crucial to understand, is that the request is for EU officials to gain control of “meta-data” from hundreds of million of mobile phone users in the region. Unlike India, the region has a comprehensive framework under the EU’s General Data Protection Regulation (GDPR) and the complementary ePrivacy Directive³⁰. This means EU authorities would be liable should the data be misused or susceptible to any data/security breach. The insights from these datasets were sought to not only track the spread of the

²⁵ The names of the telecom service providers are as follows: Deutsche Telekom in Germany; Telecom Italia, Vodafone and WindTre in Italy; and A1 Telekom Austria Group.

²⁶ Elvira Pollina and Douglas Busvine, *European Mobile Operators share data for coronavirus fight*, Reuters, March 2020, <https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2>.

²⁷ Elvira Pollina and Douglas Busvine, *European Mobile Operators share data for coronavirus fight*, Reuters, March 2020, <https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2>.

²⁸ The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>.

²⁹ Politico. *Commission tells carriers to hand over mobile data in coronavirus fight*, 2020. <https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/>

³⁰ Although a new ePrivacy Regulation is in the works; See <https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/>.

virus (on a daily basis) but to also forecast regions which would have a greater need for medical supplies.³¹

14. In contrast to the practices regions like Lombardy, the European Commission effort does not appear it will be used for compliance with containment measures. This mass database of aggregated and anonymised data will be controlled at the level of the EU bloc. The nature of data is likely to be similar to the types of data telecom operators are already sharing with national authorities in Europe. Similar aggregate level anonymised location information has been shared by Telenor in Norway, for instance.³² However, the prominent issues with many of these efforts is the questionable legal basis of these state requests. The issue with these extra legal arrangements is that they take place with no transparency with respect to the amount of data being shared, whether it is individualised or aggregated, what is the exact duration of these arrangements, what is the protocol for data retention and data sharing within government, and whether the access granted is for metadata or real-time granular insights.
15. Here, it may be prudent to reference a recent statement of the European Data Protection Board (EDPB) on the processing of personal data in the context of the COVID-19 outbreak. It states that that even though the control and eventual defeat of the pandemic is a shared goal across global communities, the processing of personal data towards the same must nonetheless protect people's personal data. The statement reads clearly saying that processing of personal data must be lawful, must be aligned with general principles of law and cannot be irreversible. Any restrictions to fundamental freedoms even in times of an emergency must be proportionate and limited to the emergency at hand.³³
16. When it comes to lawful processing, the EDPB addresses the processing of telecom data including location data. In this context, the EDPB statement refers to the need for adherence with national laws which implement the region's ePrivacy Directive. Critically, the statement highlights the principles that location data can only be used by telecom operators once it has been made anonymous or with the consent of the concerned individuals.

³¹ Politico. Commission tells carriers to hand over mobile data in coronavirus fight, 2020. <https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/>.

³² Politico. Commission tells carriers to hand over mobile data in coronavirus fight, 2020. <https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/>.

³³ *Statement on the processing of personal data in the context of the COVID-19 outbreak*. Adopted on 19 March 2020, European Data Protection Board, March 2020, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

17. It also highlights that nonetheless Article 15 of the ePrivacy Directive grants States the power to introduce legislative measures which allow for the processing of telecom data in pursuance of public security. These exceptions must nevertheless be necessary, appropriate and proportionate for a democratic society. The EDPB also clarifies that such a measure must be strictly limited to the duration of the emergency.³⁴
18. The EDPB clarifies that the onus is on public authorities to “*process location data in an anonymous way*” which helps generate reports on the concentration of mobile devices in a particular location. Article 15 of the ePrivacy Directive (referenced above) states that should governments process non-anonymised location data (allowed in limited circumstances) there is an obligation to establish adequate safeguards. An example of this is affording individuals a right to judicial remedy.

Case study 2: Asia

19. In Asia, we observe that governments are adopting a sophisticated bouquet of surveillance technologies to map the movements of infected and suspected individuals. For example, in South Korea³⁵ the government is accessing more than just cell phone location or GPS coordinates. Its government posts a “travel log” of confirmed patients in the period before they were diagnosed.³⁶ The primary aim of this programme is to “*establish virus transmission chains*”.³⁷
20. South Korea’s programme may be characterised as a 360 degree real time monitoring framework through the use of multiple technologies. It detects the movements of people confirmed or suspected to have the virus. They do this by (1) integrating existing databases/platforms; (2) tracking CCTV footage; (3) tracking credit card transaction histories; and (4) mapping location histories including GPS. These data points are collated and published for the public to

³⁴ Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020, European Data Protection Board, March 2020, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

³⁵ The New York Times. As Coronavirus Surveillance Escalates, Personal Privacy Plummets, 2020. <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>.

³⁶ Steve Hendrix and Ruth Eglash, Israel is using cellphone surveillance to warn citizens: You may already be infected, Washington Post, March 2020, https://www.washingtonpost.com/world/middle-east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

³⁷ The New York Times. As Coronavirus Surveillance Escalates, Personal Privacy Plummets, 2020. <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>.

access in an unregulated fashion. Reports suggest that the granularity of the insights collected from targeted individuals include³⁸:

- The time when they left their homes;
- Whether they wore face masks or not while using public transport;
- Stations on the subway in which they entered and exited,
- Names of clinics, shops and establishments (including bars/restaurants) that they may have visited.

21. Such insights when released to the public naturally lead to mass ostracisation and harassment which the surveilled individuals must endure. As a result South Korea's Centers for Disease Control has indicated that it intends to refine data sharing guidelines to balance privacy risks with the public interest.

22. Taiwan is another state which has been liberal in its use of surveillance technologies in combating the coronavirus. Given its proximity to the point of first discovery of the disease, Taiwan has been lauded globally for its effective action to mitigate the spread of the disease. We observe that Taiwan has actively monitored mobile networks to enforce home quarantine guidelines for at-risk individuals. The system is designed to alert police if a phone appears to be active outside the confines of the individual's designated home address. Additionally, police call these people twice daily to ensure the phone remains on the person and people do not circumvent the system by leaving the device at home.³⁹ This notion of 'electronic fencing' is becoming increasingly popular across government agencies internationally and in India, as seen in states like Tamil Nadu and Karnataka.

23. Hong Kong has a system, where persons under quarantine are given location-tracking wristbands which they must wear. Thailand also has a mobile app that anyone arriving into an airport must download. The app monitors where they visit in case they end up being diagnosed with the virus. Similarly, reports suggest that the Vietnamese capital of Hanoi has also introduced a mobile application to track cases, and possibly used to enforce quarantines.⁴⁰

24. Among other things, Singapore's Ministry of Health has a website on which it publishes information including age, gender, occupation and places travelled by

³⁸ The New York Times. As Coronavirus Surveillance Escalates, Personal Privacy Plummets, 2020. <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>.

³⁹ Reuters. Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring, 2020. <https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK>.

⁴⁰ Reuters. Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring, 2020. <https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK>

all its patients.⁴¹ The level of detail published by the city-state authorities has evoked concerns, as it goes down to publishing details with respect to interpersonal relationships. These strategies are combined with its use of a Bluetooth based contact tracing application called *TraceTogether*.⁴² We analyse the *TraceTogether* application in detail in later sections of this paper.

Case study 3: Israel

25. Israel's⁴³ usage of surveillance of location data has been described as the “most far-reaching step yet by a government in deploying the vast surveillance power that access to cellphone data provides”.⁴⁴ Israel's Prime Minister announced that the Government would employ advanced digital monitoring tools, primarily used for counter terrorism, to track disease carriers and contain the spread of COVID-19. The measure was meant to allow the Israel Security Agency (ISA or “Shin Bet”) to access “technological data” which is essentially a vague term which can capture a broad suite of metadata (and may not be confined to cellular location tracking). A concurrent measure was announced to allow the Israel Police to access location data⁴⁵.
26. Two days later the Government passed two distinct coronavirus emergency regulations (without approval of its Knesset) to reflect the aforementioned capabilities. A concerning pattern is that the regulations allow the Israel Police

⁴¹ Steve Hendrix and Ruth Eglash, *Israel is using cellphone surveillance to warn citizens: You may already be infected*, Washington Post, March 2020, https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

⁴² The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>.

⁴³ Noa Landau, *In Dead of Night, Israel Approves Harsher Coronavirus Tracking Methods Than Gov't Stated*, Haaretz, March 2020, <https://www.haaretz.com/israel-news/.premium-cellphone-tracking-authorized-by-israel-to-be-used-for-enforcing-quarantine-orders-1.8681979>.

⁴⁴ Steve Hendrix and Ruth Eglash, *Israel is using cellphone surveillance to warn citizens: You may already be infected*, Washington Post, March 2020, https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

⁴⁵ Amir Cahane, *The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers*, Lawfare, March 2020, <https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers>.

track people's cell phones without the need for a court order⁴⁶. Court orders are typically required in Israel for any surveillance/interception since such measures by the state constitute an invasion of privacy.⁴⁷ Notably, the Israel Police is also not allowed to monitor people's location in a continuous manner to enforce quarantine directives. However, a carve out does subsist to map quarantine compliance through randomised "sampling".

27. The Shin Bet or ISA is only authorized to use the data and any information derived from it only to assist the Ministry of Health (and no other government department) in conducting epidemiological investigations.⁴⁸ The nature of the data to be shared with the Ministry of Health remains unclear (probably by design). This data may be used by the Health Ministry to contact people if they were found to be in close proximity to an infected person. The regulation states that the data collected has a strict purpose limitation and cannot be used for any other purpose, including for criminal proceedings⁴⁹. It also has a strict time limitation and must be deleted within 30 days. The regulations are not to be used by Israeli authorities to access people's text messages or emails. Moreover, the ISA cannot use this data/information collected to enforce quarantine orders.
28. The Shin Bet must report all activities to Israel's Attorney General when law enforcement activities implicate people's right to privacy. Along the lines of an ordinance in India, the Israeli Government will seek to get Parliamentary approval for its regulations once the Knesset resumes. The Shin Bet will be allowed to deploy these advanced digital monitoring tools to track infected persons and will also have access to systems to track confirmed patients for a two-week period prior to being diagnosed.

⁴⁶ Amir Cahane, *The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers*, Lawfare, March 2020, <https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers>.

⁴⁷ Noa Landau, *In Dead of Night, Israel Approves Harsher Coronavirus Tracking Methods Than Gov't Stated*, Haaretz, March 2020, <https://www.haaretz.com/israel-news/.premium-cellphone-tracking-authorized-by-israel-to-be-used-for-enforcing-quarantine-orders-1.8681979>.

⁴⁸ Amir Cahane, *The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers*, Lawfare, March 2020, <https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers>.

⁴⁹ Although the regulations do not indicate punishment if this requirement is violated by authorities.

29. Notably, Israel's High Court of Justice⁵⁰ intervened and issued an interim order in the matter of *Ben Meir v Prime Minister of Israel* which limited the Shin Bet's powers and directed it to operate with parliamentary oversight. At the same time the High Court also used the interim order to forbid the Police from undertaking location surveillance under this framework, until further notice. Additionally, Israel's High Court of Justice read down the ISA Emergency Coronavirus Regulations deciding that it can only be applicable to confirmed carriers and not to individuals who were determined to be carriers by doctors (without a positive test result).⁵¹

Case study 4: United State of America

Government

30. In the US there is a conscious fear that any new system which facilitates a temporary infringement of privacy runs the risk of becoming permanent if left unaudited.⁵² At the same time, the US Government is reviewing formal options at its disposal to leverage location data held by large tech companies like Google and Facebook. However, given its own history with the collection and use of metadata by the state as outlined in the 2013 Snowden revelations, reports suggest that the state is considering strategies which can provide appropriate safeguards for people's privacy.⁵³

31. A prominent report in the Wall Street Journal in late March 2020, suggests that the US Government is analysing smartphone location data (stripped of personal information like the name of a phone's owner). The report indicates this information is being supplied by mobile advertising companies. It must be said that the degree to which this data is re-identifiable or remains susceptible to any

⁵⁰ Times of Israel, *High Court says virus mass surveillance can't continue without Knesset oversight*, March 2020, <https://www.timesofisrael.com/high-court-says-virus-mass-surveillance-cant-continue-without-knesset-oversight/>.

⁵¹ Amir Cahane, *The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers*, Lawfare, March 2020, <https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers>.

⁵² Casey Newton, *The US Government should disclose how it is using location data to fight coronavirus*, The Verge, March 2020, <https://www.theverge.com/2020/3/31/21199654/location-data-coronavirus-us-response-covid-19-apple-google>.

⁵³ Steve Hendrix and Ruth Eglash, *Israel is using cellphone surveillance to warn citizens: You may already be infected*, Washington Post, March 2020, https://www.washingtonpost.com/world/middle-east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

personal data breach remains unknown. Reportedly, the plan is to create a portal (from over 500 cities) where federal, state and local authorities can track countrywide geolocation data. The purpose for this initiative is to determine what public spaces are still attracting large crowds of people to the detriment of social distancing imperatives. This data is being shared with its Federal Centers for Disease Control.⁵⁴

32. It is speculated that the reason American authorities have sought to extract location data from mobile advertisers, as opposed to telecom operators, is because telecom operators have greater regulation with respect to data privacy. The alternative path allowed the US Government to circumvent the need for any individual consent, in which they got access to data which is accessed by advertisers through platforms like Facebook.
33. A recent article on *The Intercept* indicated that these insights were shared by an advertising technology firm called Phunware.⁵⁵ Phunware offers developers a solution which if integrated into an application allows developers to follow its users' location histories. Although the accuracy of its software has been questioned, the firm is also reportedly considering building a geo fencing solution for the US Government toward enforcement of social distancing policies.⁵⁶
34. Another example worth mentioning pertains to Palantir, a data mining company known for its work with various government agencies. According to various reports, the firm has already started with working with health authorities in both the US and the UK to model the spread of the coronavirus and anticipating hospital needs. It is building these models by getting access to anonymised data from hospitals, lab results, equipment supplies, and other healthcare data which is collated on a platform called *Palantir Foundry*. This analytics offering is also being shopped around other authorities across the world in countries like France, Germany, Switzerland and Austria. Civil society organisations like the Electronic Frontier Foundation (EFF) have stated that such arrangements

⁵⁴ Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall Street Journal, March 2020, <https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202>.

⁵⁵ Sam Biddle and Lee Fang, *Location-Tracking Firm Helping Trump Get Reelected Now Wants to Cash in on Coronavirus*, *The Intercept*, April 2020, https://theintercept.com/2020/04/09/coronavirus-trump-smartphone-tracking/?utm_medium=email&utm_source=The%20Intercept%20Newsletter

⁵⁶ Sam Biddle and Lee Fang, *Location-Tracking Firm Helping Trump Get Reelected Now Wants to Cash in on Coronavirus*, *The Intercept*, April 2020, https://theintercept.com/2020/04/09/coronavirus-trump-smartphone-tracking/?utm_medium=email&utm_source=The%20Intercept%20Newsletter

between government and private sector, which arise out of the pandemic require close scrutiny.⁵⁷

Non-government

35. There is an emergent trend wherein contact tracing and location based surveillance is gradually increasing via large technology platforms and vendors. For instance, Google is using location data in smartphones to publish community level mobility reports.⁵⁸ These reports show aggregated and anonymised insights. Compiled insights are based on people who have “opted in” to sharing their location histories with Google. It essentially uses similar technologies/systems to what Google uses for its Maps application which shows users insights such as the level of traffic on a particular route.
36. Each country’s mobility report shows patterns according to six categories including: (1) Retail and recreation; (2) Grocery and Pharmacy; (3) Parks and Public Spaces; (4) Transit Stations; (5) Workplaces; and (6) Residences. Separately, Google has previously been considering projects in which it plans to use similar anonymised aggregated datasets and systems to “forecast the path of the pandemic”.⁵⁹ The actual efficacy of such high-level mobility trends in disease control has been questioned.⁶⁰ Apart from questionable utility, civil society activists have suggested that such data aggregation practices can have underlying privacy risks. Therefore, the manner in which such datasets have been collated, the assumptions made therein and the systems of analysis should be published transparently so that it is auditable by the public.⁶¹

⁵⁷ Taylor Hatmaker, *Palantir provides COVID-19 tracking software to CDC and NHS, pitches European Health Agencies*, Tech Crunch, April 2020, <https://techcrunch.com/2020/04/01/palantir-coronavirus-cdc-nhs-gotham-foundry/>.

⁵⁸ COVID-19 Community Mobility Reports, Google, 2020, <https://www.google.com/covid19/mobility/>.

⁵⁹ Casey Newton *Google uses location data to show which places are complying with stay at home orders-- and which aren't*, The Verge, April 2020, <https://www.theverge.com/2020/4/3/21206318/google-location-data-mobility-reports-covid-19-privacy>.

⁶⁰ Casey Newton *Google uses location data to show which places are complying with stay at home orders-- and which aren't*, The Verge, April 2020, <https://www.theverge.com/2020/4/3/21206318/google-location-data-mobility-reports-covid-19-privacy>.

⁶¹ Natasha Lomas, *Google is now publishing coronavirus mobility reports, feeding off users' location history*, Tech Crunch, April 2020, <https://techcrunch.com/2020/04/03/google-is-now-publishing-coronavirus-mobility-reports-feeding-off-users-location-history/>.

37. Along similar lines, researchers in the US have used location data from Facebook to measure social distancing in California. In March 2020, one researcher used anonymised location data held by Facebook to build an aggregate mapping tool under Facebook's *Data for Good* programme which tracks population movements during natural disasters and disease outbreaks.⁶² What is interesting is that around 125 not for profits across the world have access to such anonymised location datasets.
38. More recently, media reports indicated that Facebook is looking to revamp its *Data for Good* programme to aid public health officials to gauge the success of social distancing programmes.⁶³ The company which has been at the centre of multiple controversies vis-a-vis people's personal data asserts that this exercise will not compromise on people's privacy. The new tools will ensure all datasets are aggregated, privacy-preserving and anonymised location data. These tools are meant to build *Disease Prevention Maps*⁶⁴, to create predictive models where outbreaks are likely to break out.
39. These tools are to be accessible by researchers and universities. The types of maps which can be built through these tools include: (a) co-location maps i.e. the probability that people may come into contact with one another, and risk areas where human to human transmission is higher; (b) Aggregate level movement and cellular coverage maps; and (c) data on whether are people staying at or near their homes. While this project is presently limited to the US, Facebook CEO Mark Zuckerberg has indicated that this feature of the *Data for Good* programme may be exported globally. The report does suggest that location data collection is contingent on users opting-in. But the mechanism described in the report suggests that the opt-in is merely with respect to the collection of location data, and not vis-a-vis the purpose⁶⁵ to which said location data is deployed.⁶⁶

⁶² Protocol. Facebook data can help measure social distancing in California, 2020.
<https://www.protocol.com/facebook-data-help-california-coronavirus>.

⁶³ Christina Farr, Facebook is developing new tools for researchers to track if social distancing is working, CNBC, April 2020,
<https://www.cnbc.com/2020/04/06/facebook-to-help-researchers-track-if-social-distancing-is-working.html>.

⁶⁴ Disease Prevention Maps, Facebook Data for Good, April 2020,
<https://dataforgood.fb.com/tools/disease-prevention-maps/>.

⁶⁵ Location data from users' check ins may be used for these experiments by researchers.

⁶⁶ Christina Farr, Facebook is developing new tools for researchers to track if social distancing is working, CNBC, April 2020,
<https://www.cnbc.com/2020/04/06/facebook-to-help-researchers-track-if-social-distancing-is-working.html>.

Limitations in location tracking

40. Experts suggest that as COVID-19 becomes entrenched within communities the usefulness of anonymised metadata from mobile phones will end. In situations of lockdown, most people are likely to confine themselves to their neighbourhoods and communities. Therefore, insights from cell towers will not be able to offer the level of detail which is relevant to track people's localised movements. With countries like Israel relying on location surveillance and not allowing citizens any agency to sign up or any opportunity to "opt out"⁶⁷, it is important to evaluate these intrusive responses through the prism of efficacy. This is because if a rights violating response does not present efficacious solutions, then its adoption for any duration may need to be reconsidered.
41. In this regard, let us consider the inputs of Professor Landau. She mentions that it is important to consider the information authorities could glean from location data, and contrast it with how COVID-19 spreads i.e. at a person to person level. Risk environments include closed indoor settings and large public gatherings. In this regard, signals pinging of cell towers tracking phones can give you a rough measure of the location of an individual. However, it cannot provide authorities with insights at the level of six foot proximities which is what is required to gauge risk levels of exposure to the virus.
42. Similarly, she highlights that GPS location data while more granular in nature suffers from poor reliability indoors. She uses the example that while the data can tell you that two individuals got into the same subway station, it is incapable of telling you if two people were in the same coach/bogie. Moreover, GPS can drain people's battery and can lead to phones shutting down which bring with it its own sets of challenges.⁶⁸ Another issue which is obvious is that people who wish to not be surveilled via their mobile devices can simply leave their phone at home and venture out.
43. Additionally, a larger concern is that the creation of new laws, systems and architectures of surveillance; or the deployment of a patchwork of surveillance technologies will enable permanent surveillance mechanisms. Key balancing considerations include strict limitations in terms of time, amount collected and the use of the data collected.

⁶⁷ Steve Hendrix and Ruth Eglash, *Israel is using cellphone surveillance to warn citizens: You may already be infected*, Washington Post, March 2020, https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

⁶⁸ Susan Landau, *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, Lawfare, March 2020, <https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters>.

How can governments allay your fears?

44. On this front this paper endorses the views of the Electronic Frontier Foundation (EFF). EFF has urged governments to demonstrate the exact way that they intend to use surveillance (in a human rights respecting manner) to fight the coronavirus. They elaborate that such disclosures must be scientifically rigorous and supported by the opinion of public health officials. EFF also urges governments to elaborate what are the rules and laws which apply to keep the government accountable. Second, governments must ensure that such plans and accompanying rationale must be put forth before the public to scrutinise. They state that there is a heightened onus to justify location surveillance since it can reveal intimate details of people's lives, and can easily be connected with people's sensitive personal information.⁶⁹ Moreover, there are new reports of Governments across the world potentially working with spyware firms like the NSO Group (known for the Pegasus spyware data breaches and linked with the murder of journalist Jamal Khashoggi) to deploy sophisticated tools to map people's movements.⁷⁰
45. Governments also need to address the risks of information security threats relating to the re-identification of de-identified/anonymised data.⁷¹ Factors such as what data points are being used for aggregation, and thresholds of aggregation must be discussed. To conclude, EFF asks a series of prescient questions which Indian decision makers must mull over when considering the deployment of location tracking mechanism:
- A. Are the location records sought sufficiently granular to show whether two people were within transmittable distance of each other? If not will location based surveillance combined with push notifications of contact, be based on accurate evidence or will it merely stir panic within the public.
 - B. Do the cell phone location records identify a representative portion of the overall population, especially those from low income groups?

⁶⁹ Adam Schwartz and Andrew Crocker, *Governments haven't shown location surveillance would contain COVID-19*, Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19>.

⁷⁰ Rory Cellan-Jones, *Coronavirus: Israeli spyware firm pitches to be COVID-19 saviour*, BBC, April 2020, <https://www.bbc.com/news/health-52134452>.

⁷¹ Adam Schwartz and Andrew Crocker, *Governments haven't shown location surveillance would contain COVID-19*, Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19>.

- C. Has the virus already spread so broadly that location tracking is no longer a significant way to reduce transmission? If yes, have such tracking activities become impractical and will they divert resources from more effective on-ground/human containment methods.
- D. Will health-based surveillance deter people from seeking health care?

5. Contact tracing apps, websites and platforms

Future of technology for disease control?

1. The above discourse may be viewed as a precursor to what is likely to be to the future of technology based interventions during this pandemic. *Prima facie*, the allure of contact tracing applications remains apparent. As succinctly demonstrated in a recent article by Susan Landau, these applications are trying to overcome the limitations of location tracking via cell phone towers and GPS coordinates. Other limitations include the fact that location-based tracking as seen with the Israeli example, or even the Delhi example, can be administered without people's consent leading to privacy and civil liberty concerns.⁷²
2. But even from an efficacy perspective, Landau highlights that the information revealed from location data pinging across cell towers or GPS data is not granular enough or reliable enough to inform an individual if they are at risk of exposure. In this context, she highlights the alternative of bluetooth beacons in contact tracing. But for it to be effective, there is a need for a sufficient percentage of the population to install a technology system deploying Bluetooth proximity solutions. If authorities start playing a proverbial game of whack-a-mole to monitor transmission, there are risks of high error rates and concomitant mistrust of government technologies.⁷³ But, first for the benefit of readers, when it comes to the coronavirus what is it that these technologies are trying to aid with?
3. According to the WHO, contact tracing occurs in three discrete steps namely (a) contact identification; (b) contact listing; and (c) contact follow up. In particular, contact tracing is a pillar which helps public health officials in containing and

⁷² Susan Landau, *Location Surveillance to Counter COVID-19: Efficacy is What Matters*, Lawfare, March 2020, <https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters>.

⁷³ Susan Landau, *Location Surveillance to Counter COVID-19: Efficacy is What Matters*, Lawfare, March 2020, <https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters>.

slowing the pace of further transmission of virus.⁷⁴ This pace of transmission is measured by the unit R_0 (R naught) which essentially connotes the number of people an infected person can spread the disease onto.⁷⁵ Contact tracing is viewed as a strategy, wherein timely interventions can breakup new infection chains.

4. Contact tracing has traditionally been administered through the use of on ground personnel and volunteer armies. However, with the ubiquity of mobile devices (including smartphones), which collect vast troves of personal information, governments across the world clearly believe surveillance can aid with rapid contact tracing, and identification of hotspots. But owing to the peculiarities of the novel coronavirus, authorities across the world are beginning to realise the limited efficacy associated with respect to location surveillance (both with cell tower data and with GPS signals).
5. As a result governments and other groups have either released or are developing smartphone apps that use Bluetooth beacons to log instances wherein a user's device comes in contact with another user's device. When a user of the app is detected to have Covid-19, contact tracing officers might be able to use the app to identify their close contacts in the prior days or weeks - contacts that the patient might be unable to recall. These apps have great promise to make contact tracing more effective and might be an important weapon in fighting this epidemic but also at the same time create the infrastructure for mass surveillance and impact democratic rights.

International development of contact tracing apps

Case Study 1: Singapore

6. As mentioned later in this report a prominent example of the use of a bluetooth based contact tracing app is the *TraceTogether* app which has been deployed in Singapore. We include an exhaustive front-end analysis of *TraceTogether* separately in Part 7 of the present working paper and address questions on deployment and efficacy here. Given Singapore's initial success in containing the spread of the virus (of course steered by rapid testing and isolation practices), the *TraceTogether* app is increasingly viewed globally as a replicable model for close proximity contact tracing. To be clear, an important lesson for decision

⁷⁴ Contact Tracing, Q&A, World Health Organisation, May 2017, <https://www.who.int/features/qa/contact-tracing/en/>.

⁷⁵ Joseph Eisenberg, *R_0 : How scientists quantify the intensity of an outbreak like coronavirus and predict the pandemic's spread*, The Conversation, February 2020, <https://theconversation.com/r0-how-scientists-quantify-the-intensity-of-an-outbreak-like-coronavirus-and-predict-the-pandemics-spread-130777>.

makers in countries like India is that Singapore does not view this technology based solution as a silver bullet.

7. The *TraceTogether* application is meant to complement existing physical contact tracing practices administered by people on the ground. One may view it as an incremental solution towards completeness of data and for rapid response/notification of users. In essence it is geared to overcome human error/slow recall of events. Rapid response is meant to drive early testing and early detection, key pillars to limit transmission.
8. The application was developed by Singapore's Government Technology Agency (GovTech) and its Ministry of Health.⁷⁶ It adopts a voluntary model where people share their information, and tracks other people in the vicinity who are confirmed via bluetooth. Once an individual tests positive for COVID-19, all people confirmed to be in that individual's vicinity in the run up to the diagnosis will be notified. Additionally, the government is also notified about this. The application adopts an opt-in model and does not track users through space (no collection or usage of location or GPS coordinates), but rather tracks who you may be in contact with. Location details may only therefore be accessed by physical contact tracers.⁷⁷
9. To register on the application, users must share their phone number to be assigned a user ID which is used to generate temporary IDs, periodically. When the phone is running the application, it requires access to both **location services** and **Bluetooth** to be on. When another phone running the application comes into range⁷⁸, there is an exchange of four discrete pieces of information:

A. Bluetooth signal strength

B. Model of phone

⁷⁶ Tang See Kit and Aqil Haziq Mahmud, *Singapore launches TraceTogether mobile app to boost COVID-19 contact tracing efforts*, Channel News Asia, March 2020, <https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616>.

⁷⁷ Tang See Kit and Aqil Haziq Mahmud, *Singapore launches TraceTogether mobile app to boost COVID-19 contact tracing efforts*, Channel News Asia, March 2020, <https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616>.

⁷⁸ According to guidelines close proximity according to the app ranges from 2 metres, to 5 metres when exposure is 30 minutes; See Tang See Kit and Aqil Haziq Mahmud, *Singapore launches TraceTogether mobile app to boost COVID-19 contact tracing efforts*, Channel News Asia, March 2020, <https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616>.

C. Temporary device level identifier

D. Time stamp

10. According to our analysis and secondary research each interaction will be recorded on people's devices. However, users are obligated to share information with the Health Ministry when requests are made during contact tracing investigations. This is important to highlight since a refusal by a user could lead to prosecution under Singapore's Infectious Diseases Act.⁷⁹
11. Given the global interest with the Singaporean model, Singapore has announced plans to open-source the *TraceTogether* source code for access by global counterparts.⁸⁰ It will also publish its research with respect to Bluetooth based proximity tracking.⁸¹ The purpose of the *TraceTogether* application is to better inform health authorities as to who must be placed in quarantine and for efficient allocation of resources.

Case Study 2: Asia

12. As has been widely discussed, the Chinese Government has an enormous technological and bureaucratic surveillance architecture. It combines app-based monitoring solutions with a suite of other surveillance technologies like Closed Circuit Television (CCTV) footage, facial recognition technologies⁸², body temperature detection⁸³ software and credit card transaction histories to piece

⁷⁹ Infection Diseases Act (Act 21 of 1976), Section 58(2), Extraordinary in relation to emergency measures, <https://sso.agc.gov.sg/Act/IDA1976>; Also see: Ministry of Health, Government of Singapore, *Two Charged under Infectious Diseases Act for false information and obstruction of contact tracing*, February 2020, <https://www.moh.gov.sg/news-highlights/details/two-charged-under-infectious-diseases-act-for-false-information-and-obstruction-of-contact-tracing>.

⁸⁰ *BlueTrace Manifesto*, Ministry of Health, Singapore & GovTech Singapore, <https://bluetrace.io/>.

⁸¹ Simon Sharwood, *Singapore to open-source national Coronavirus encounter-tracing app and the Bluetooth research behind it*, The Register, March 2020, https://www.theregister.co.uk/2020/03/26/singapore_tracetogether_coronavirus_encounter_tracing_app_lessons/

⁸² Martin Pollard, *Even Mask-Wearers Can Be ID'd, China Facial Recognition Firm Says*, Reuters, March 2020, <https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL>; Dave Gershgor, *Facial Recognition Companies See the Coronavirus as a Business Opportunity*, One Zero | Medium, March 2020, <https://onezero.medium.com/facial-recognition-companies-see-the-coronavirus-as-a-business-opportunity-6c9b99d60649>.

⁸³ *Recommendations on Privacy and Data Protection in the Fight Against COVID-19*, Access Now, March 2020,

together the movements of infected persons. These technology based mechanisms are being complemented by human-based means of surveillance like neighbourhood committees to track the direction and spread of the virus.⁸⁴ The combination of these systems demonstrate the magnitude and depth of state coercion it is deploying to control human behaviour during the pandemic. But to replicate that coercion other governments may have to build new systems to match these capabilities and outcomes. Its alignment with democratic principles remains untenable.

13. For instance, people in China are required to use software which analyses a suite of data points to generate automated classifications with a colour code of red, yellow or green to depict contagion risk. The software (called the Alipay Health Code connected with the popular Alipay wallet service⁸⁵) also makes decisions with respect to whether people should quarantine themselves, or be allowed to use public transport, enter malls or any public space. According to a report by the *New York Times*,⁸⁶ the software shares real time information with the police, without any hint of a framework providing safeguards. The decision making criteria and process for how people are assigned colours has not been revealed to the public.
14. The system has been rolled out in more than 200 cities and is set for nation-wide expansion. According to the analysis undertaken by NYT, when a user grants the software access to its location, the person's location along with city name and an identifier is captured in a piece of the programme and shared with a server which is accessible by the police. The system relies on accessing information about known coronavirus patients, government-held data on people's travel bookings. Another major platform provider Tencent, which runs the popular WeChat, is said to be building a similar platform for coronavirus related surveillance. No transparency with how these systems are used leads to concerns of abuse and possible discrimination between communities.⁸⁷

<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>.

⁸⁴ Steve Hendrix and Ruth Eglash, *Israel is using cellphone surveillance to warn citizens: You may already be infected*, Washington Post, March 2020, https://www.washingtonpost.com/world/middle-east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

⁸⁵ Developed by Ant Financial which is a sister concern of e-commerce juggernaut Alibaba.

⁸⁶ Paul Mozur and others, *In Coronavirus fight, China gives citizens a color code, with red flags*, New York Times, March 2020, <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>.

⁸⁷ Paul Mozur and others, *In Coronavirus fight, China gives citizens a color code, with red flags*, New York Times, March 2020, <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>

15. These applications are so powerful that it is only after these applications give a 'green clearance', are people allowed to reenter public spaces and move around freely.⁸⁸ Russia is another country which is using facial recognition systems. The police in Moscow have reportedly used such systems to arrest people who violate quarantine orders.⁸⁹ In South Korea, where widespread testing and stringent quarantine procedures have proven effective so far, another key aspect of its COVID-19 containment strategy is a central contact tracing mobile application called Corona 100m.⁹⁰ The application is designed in a manner to inform users if they were within 100 metres of a known case.
16. While Israel may not fall uniquely within Asia, we have also covered it in this section given similarity in the functionality with other existing deployments in the region. Israel, which we have already discussed in the context of location tracking, has also released a voluntary contact tracing/monitoring application called HaMagen.⁹¹ The application has been developed and its source code has been published on Github, affording other countries the opportunity to build plug and play models for themselves. It is suggested that people's personal and location data is stored locally on people's devices. This data is compared with information which is stored by the Israeli Health Ministry servers. Upon being notified about exposure people may voluntarily report to the Government that they have possible exposure to the virus through the application.⁹²

⁸⁸ Recommendations on Privacy and Data Protection in the Fight Against COVID-19, Access Now, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>.

⁸⁹ Sam Biddle, Privacy Experts Say Responsible Coronavirus Surveillance is Possible, The Intercept, April 2020, <https://theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/>.

⁹⁰ Alexis Dudden and Andrew Mark, South Korea took rapid, intrusive measures against COVID-19 and they worked, The Guardian, March 2020, <https://www.theguardian.com/commentisfree/2020/mar/20/south-korea-rapid-intrusive-measures-covid-19>.

⁹¹ Allison Kaplan Sommer, Israel Unveils Open Source App to Warn Users of Coronavirus Cases, Haaretz, March 2020, <https://www.haaretz.com/israel-news/israel-unveils-app-that-uses-tracking-to-tell-users-if-they-were-near-virus-cases-1.8702055>.

⁹² Tova Cohen, 1.5 million Israelis using voluntary coronavirus monitoring app, April 2020, <https://www.reuters.com/article/us-health-coronavirus-israel-apps/1-5-million-israelis-using-voluntary-coronavirus-monitoring-app-idUSKBN21J5L5>.

Case Study 3: Europe

17. Other reports suggest that countries like the US⁹³, UK⁹⁴ and Germany are also contemplating developing contact tracing apps to track the spread of the virus. For instance, the UK's National Health Service (NHS) is reportedly working with a subsidiary of software firm VMware (Pivotal) to develop a Bluetooth based contact tracing application.⁹⁵ In particular Germany⁹⁶, which is aiming to launch a smartphone application is reliant on Singapore's *TraceTogether* approach whilst preserving people's individual privacy. Given its fraught history with surveillance, Germans are culturally deeply suspicious of excessive surveillance powers being granted to the state, even if access to say location data may help with swift mapping of the pandemic.
18. Like Singapore, reports suggest that senior government officials in Germany⁹⁷ are in agreement with respect to mapping close-proximity Bluetooth 'handshakes' between smartphones. The application is being developed by the *Fraunhofer Heinrich Hertz Institute for telecoms* (HHI), a primary institution of applied scientific research. Reports suggest that it is working with counterparts across Europe to develop a standard for such apps where information such as (a) proximity; and (b) duration of contact will be stored locally on people's phones for a period of two weeks. These details are also meant to be stored anonymously and without the use of location data.⁹⁸ Experts suggest that privacy respecting

⁹³ Rachel Shabi, *UK missed coronavirus contact tracing opportunity, experts say*, The Guardian, April 2020, <https://www.theguardian.com/uk-news/2020/apr/06/uk-missed-coronavirus-contact-tracing-opportunity-experts-say>.

⁹⁴ Thomas Macaulay, *New coronavirus contact-tracing app coming to UK 'within weeks'*, The Next Web, April 2020, <https://thenextweb.com/neural/2020/04/01/new-coronavirus-contact-tracing-app-coming-to-uk-within-weeks/>.

⁹⁵ Hannah Murphy, *US and Europe race to develop 'contact tracing' apps*, Financial Times, April 2020, <https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95>.

⁹⁶ Reuters, *Germany aims to launch Singapore style Coronavirus app in weeks*, New York Times, March 2020, <https://www.nytimes.com/reuters/2020/03/30/technology/30reuters-health-coronavirus-germany-tech.html>

⁹⁷ Reuters, *Germany aims to launch Singapore style Coronavirus app in weeks*, New York Times, March 2020, <https://www.nytimes.com/reuters/2020/03/30/technology/30reuters-health-coronavirus-germany-tech.html>

⁹⁸ Reuters, *Germany aims to launch Singapore style Coronavirus app in weeks*, New York Times, March 2020, <https://www.nytimes.com/reuters/2020/03/30/technology/30reuters-health-coronavirus-germany-tech.html>

contact tracing can be effective in relaxing stringent lockdown/curfew conditions.

Pan-European Privacy-Preserving Proximity Tracing Project

19. Germany's HHI has led a coalition of European technologists and experts to develop the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project.⁹⁹ So far in Europe the primary purpose of mobile phone applications in the fight against coronavirus include contact tracing, lockdown/quarantine enforcement and COVID-19 self assessments. The PEPP-PT project leans on the idea that technology should be able to notify individuals if they have come in close contact with another infected person. This assessment can be done via proximity settings wherein two mobile devices can essentially 'talk to one another' without the need for an external arbiter. This is done when two phones are in Bluetooth proximity with one another administering what is commonly referred to as a Bluetooth handshake.¹⁰⁰
20. The standards developed by the PEPP-PT appear essential since the region is seeing multiple applications sprout up-- something a country like India can relate to. Moreover, considering the globalised nature of the coronavirus, from an efficacy standards it would be desirable if such applications were interoperable with one another. Therefore, standards are being erected to ensure that there is a semblance of consistent privacy-respecting technology being deployed across the region. As mentioned earlier, the region has tight privacy controls under the GDPR and its ePrivacy Directive. The PEPP-PT standard also appears novel since there is no attempt to collect location data, no movement profiles, no contact information, and zero device related identification markers.¹⁰¹
21. Apps adhering to this standard are only expected to generate temporary IDs-- to avoid identifying specific individuals. This allows devices which use the app to exchange these temporary IDs with one another and store them locally in an encrypted format. Should an individual test positive, then the individual's doctor may request them to transfer their contact list into a central server. These contacts would then be notified and would then have an opportunity to

⁹⁹ <https://www.pepp-pt.org/>

¹⁰⁰ Natasha Lomas, *An EU Coalition of techies is backing a 'privacy-preserving' standards for COVID-19 contacts tracing*, Tech Crunch, April 2020, <https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/>.

¹⁰¹ Natasha Lomas, *An EU Coalition of techies is backing a 'privacy-preserving' standards for COVID-19 contacts tracing*, Tech Crunch, April 2020, <https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/>.

self-isolate and/or get tested. The PEPP-PT also provides for opportunities for API integration to build solutions on its protocols. It also offers a certification process to ensure local-level implementation is in compliance with the standard.

102

22. At the same time, there remain concerns about the level of re-identification risk which subsist when anonymised datasets are indeed transferred to a central server as suggested by the PEPP-PT standard.

Views of regional European authorities

23. As such the European Data Protection Supervisor (EDPS) recently noted, effective anonymisation “*requires more than removing obvious identifiers such as phone numbers and IMEI numbers*”.¹⁰³ On a related note the EDPS recently noted that instead of running the risk of multiple contact tracing apps wherein a multiplicity of apps can represent a threat to people’s individual privacy, there is a case for a EU-wide contract tracing mobile application.¹⁰⁴ The EDPS stated that any such app should deploy temporary broadcast identifiers along with close range bluetooth technologies, which would allow it to be compliant with people’s privacy protections under data protection frameworks.

Case Study 4: Latin american approaches

24. In Latin America, Privacy International’s (PI’s) repository on apps being developed for COVID-19 is instructive.¹⁰⁵ For instance, Argentina’s ‘voluntary’ self-diagnosis web app which has been developed by its Secretariat of Public Innovation asks users to mandatorily share comprehensive reams of information including their national ID number, phone number and email address. The Android version of the app seeks permissions to people’s calendar, contacts, geolocation data (which includes network and GPS). Argentina’s Public Prosecutor office is also mandating the installation of an application on the

¹⁰² Natasha Lomas, *An EU Coalition of techies is backing a ‘privacy-preserving’ standards for COVID-19 contacts tracing*, Tech Crunch, April 2020, <https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/>.

¹⁰³ WOJCIECH RAFAŁ WIEWIÓROWSKI, *Monitoring Spread of COVID-19*, European Data Protection Supervisor, March 2020, https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.

¹⁰⁴ Foo Yun Chee, *EU Privacy Watchdog calls for pan-European mobile app for virus tracking*, Reuters, April 2020, <https://www.reuters.com/article/us-health-coronavirus-tech-privacy/eu-privacy-watchdog-calls-for-pan-european-mobile-app-for-virus-tracking-idUSKBN21O1KJ>.

¹⁰⁵ Apps and COVID-19, Privacy International, 2020, <https://privacyinternational.org/examples/apps-and-covid-19>

phones of people who have violated government issued quarantine directives in certain cities.¹⁰⁶

25. In Colombia, the Government has repurposed an old app (which was used for the 2016 Rio Olympics) and rebranded it *Coronapp*. Privacy International describes the nature of personally identifiable information which the app collects including full name, ethnicity, date of birth, email address and whether they attended any mass public events in a defined timed period. The request to access such information, as a prerequisite to even use the app, remains controversial since the country was in the midst of large political protests. It was viewed as a way to identify dissenters against the establishment. The app's terms and conditions fails to sufficiently clarify how this data collected would be used or protected.¹⁰⁷

Surveillance firms eye profit & reputation laundering

26. While it is useful to track how governments are initiating such projects, we must also track the role of private sector firms in proliferating surveillance systems during this public health crisis. One such example is the NSO Group Ltd, an Israeli cybersecurity firm which is known to supply spyware technologies to government agencies-- typically law enforcement. NSO Group has found its name mentioned in various incidents relating to alleged human rights violations. For instance, their technologies were connected with the murder of journalist Jamal Khashoggi.¹⁰⁸ Second, in the Indian context, they were identified as the suppliers of the Pegasus spyware which was used to hack the VOIP protocol of WhatsApp through which the phones of Indian lawyers and civil society activists were hacked.¹⁰⁹
27. In this context, the NSO Group is developing a software to support governments in tracking the spread of the coronavirus. The software, which is being allegedly tested by around a dozen countries, takes two weeks of mobile-phone tracking

¹⁰⁶ Argentina mandates app installation for quarantine breakers, Privacy International, March 2020, <https://privacyinternational.org/examples/3568/argentina-mandates-app-installation-quarantine-breakers>.

¹⁰⁷ Colombia: Coronapp fails at public information purpose, Privacy International, March 2020, <https://privacyinternational.org/examples/3435/colombia-coronapp-fails-public-information-purpose>.

¹⁰⁸ The New York Times. Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says, 2020. <https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html>.

¹⁰⁹ Sanyukta Dharmadhikari, *The Indian activists, lawyers snooped on through WhatsApp by Israeli spyware Pegasus*, The News Minute, October 2019, <https://www.thenewsminute.com/article/indian-activists-lawyers-snooped-through-whatsapp-israeli-spyware-pegasus-111506>.

information from an infected person, and then this is compared with corresponding location data which is collated from telecom service providers. Such a system allows this reported software to identify vulnerable individuals who would have been in the patient's vicinity for a period of 15 minutes or more.

110

28. This particular product is reportedly being packaged as a civilian product and is being sold to National Health Ministries. The technology is such that should it detect a risk for any infection, a text message will be shared to a particular sim number without revealing the same to authorities. Authorities will only be allowed to correlate these details with a person's identity with the consent of an individual who has tested positive for the coronavirus.¹¹¹ These trends are not unique to global surveillance firms. Indian firms such as those heavily invested in the development of facial recognition technologies such as Innefu Labs and FaceTaggr have posed technology based surveillance as solutions to the government.

Development of contact tracing interventions in India

Committee for developing a citizen app technology platform

29. When it comes to using applications for COVID-19 response, Indian authorities are eagerly following suit. On April 03, 2020 the Secretary of India's Ministry of Human Resource Development (MHRD) issued a notification¹¹² which formally acknowledges the Government's new contact tracing application which is available via iTunes for iOS, and via Play Store for Android. On the same day i.e. April 03, 2020, India's Cabinet Secretariat issued another notification.¹¹³ It announced the *Constitution of a Committee for developing and implementing a Citizen app technology platform for combating COVID-19*.
30. The notification states that developing a nation-wide technology which onboards all citizens can be instrumental in combating the pandemic. The Committee will seek to create an "enabling mechanism" through a PPP model to

¹¹⁰ Gwen Ackerman and Yaacov Benmeleh, *Israeli Spyware firm wants to track data to stop coronavirus spreading*, Bloomberg, March 2020, <https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus>.

¹¹¹ Gwen Ackerman and Yaacov Benmeleh, *Israeli Spyware firm wants to track data to stop coronavirus spreading*, Bloomberg, March 2020, <https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus>.

¹¹² D.O. No. Secy (HE)/MHRD/2020, Department of Higher Education/School Education & Literacy, Ministry of Human Resource Development, April 03 2020.

¹¹³ F. No. 101/2/1/2020-CA.IV, Cabinet Secretariat, Government of India, April 03 2020.

develop and implement a Citizen app platform. It aims to onboard all citizens to fight the pandemic, and also evaluate/converge related technology solutions towards the platform. The Committee comprises:

- a. TRAI Chairperson; Mr RS Sharma
 - b. Principal Scientific Advisory to Government of India; Professor K Vijay Raghavan;
 - c. Meity, Secretary; Mr Ajay Prakash Sawhney
 - d. DoT Secretary; Mr Anshu Prakash
 - e. Mahindra & Mahindra Chairperson; Mr Anand Mahindra
 - f. Tata Sons, Chairperson; Mr N Chandrasekaran
 - g. Member, NSAB, IIT Chennai; Professor V Kamakoti
31. The Ministry of Electronics and Information Technology (MeitY) has been entrusted with the responsibility to provide secretarial support to the Committee. It will also receive assistance from the Prime Minister's Office's Deputy Secretary, Mr Manharsinh Yadav. The Committee also has the flexibility to co-opt other members as per requirements. The Committee must complete its work within a three month period which means it must deliver on its mandate by July 03, 2020

Prior projects by the Government of India

32. It is noticeable that this Committee lacks any representation from the Ministry of Health and Family Welfare (MoHFW), or any independent involvement of persons with a medical or epidemiological background. The exact nature of work that the Committee will undertake remains unclear since the Government has already launched the *Aarogya Setu* app for mobile devices operating on Android and iOS. Prior to this, the Government had launched another contact tracing application called *Corona Kavach*. This particular version was not widely available and a beta version was released only for Android devices.¹¹⁴
33. Another report on the *Economic Times* suggested that both MeitY and NITI Aayog (India's nodal policymaking arm) were separately developing contact tracing apps in response to COVID-19. Even as both departments were undertaking technical development, the same report indicated that a Committee was still studying the contours of the eventual app. It also suggested that both apps were in the beta testing phase and being studied by the Committee. The

¹¹⁴ Darab Mansoor Ali, *Corona Kavach is Government's New Location-based COVID-19 Tracking App: This is How You Use It*, NDTV, March 2020, <https://gadgets.ndtv.com/apps/news/covid-19-tracker-corona-kavach-government-of-india-coronavirus-how-to-use-2201703>.

Committee decided that a nodal app should combine features from both the MeitY app and the NITI Aayog app.¹¹⁵

34. A recent report on the *Indian Express* confirmed that NITI Aayog, led a team of different entities. This included working with the National Informatics Centre (NIC) and a series of technologist volunteers on this project.¹¹⁶
35. These contract tracing apps were being designed with a view to help in notifying users if they crossed paths with someone who had tested positive for COVID-19. The Corona Kavach app which was being beta tested by MeitY was reportedly inspired by the South Korean government app called Corona 100m. The Corona Kavach app was designed to use (1) the phone number of the user; (2) location data of the smartphone; and (3) map this data against location data of infection patients which is held by the Indian Council of Medical Research (ICMR). For closer range location tracking, the Corona Kavach app was meant to also use Bluetooth signals along the lines of Singapore's *TraceTogether* app.¹¹⁷
36. At the same time, the app being developed by NITI Aayog, was reportedly beta tested on both Android and iOS, with at least 10 thousand users. Another report described this app, named Cowin-20, as "more advanced" than Corona Kavach. Cowin-20 reportedly used location and bluetooth access to determine accurate proximity between users.¹¹⁸ In another instance, a private sector firm called Innefu, reportedly created an app called *Unmaze* to help inform authorities if individuals are observed to breach quarantine orders. The same report confirms that the app is being offered to authorities for free and at least three police departments across the country are using *Unmaze* to tackle the virus.¹¹⁹ Geo location apps are also seen as an opportunity to provide useful aggregated

¹¹⁵ Venkat Ananth, *Government likely to launch COVID path-tracing app*, The Economic Times, March 2020, <https://economictimes.indiatimes.com/tech/software/govt-likely-to-launch-covid-path-tracing-app/articleshow/74819186.cms>.

¹¹⁶ Karishma Mehrotra, *Behind Aarogya Setu app push: 'At least 50% people must download for impact'*, Indian Express, April 2020, <https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/>.

¹¹⁷ Venkat Ananth, *Government likely to launch COVID path-tracing app*, The Economic Times, March 2020, <https://economictimes.indiatimes.com/tech/software/govt-likely-to-launch-covid-path-tracing-app/articleshow/74819186.cms>.

¹¹⁸ Prasad Banerjee, *India taps location surveillance apps to keep virus in check*, Live Mint, March 2020, <https://www.livemint.com/technology/tech-news/india-turns-to-location-surveillance-to-contain-spread-of-covid-19-11585466140031.html>.

¹¹⁹ Prasad Banerjee, *India taps location surveillance apps to keep virus in check*, Live Mint, March 2020, <https://www.livemint.com/technology/tech-news/india-turns-to-location-surveillance-to-contain-spread-of-covid-19-11585466140031.html>.

insights and motion flow analysis to authorities to inform future resource allocation decisions. These insights can be used by authorities and relief groups to make determinations like which testing centres are suffering from excessive demands and testing requests. The data for such mapping technologies (built by the private sector) are sourced from Government authorities. The National Informatics Centre's (NIC's) Bharat Maps platform is one such repository.¹²⁰

37. These solutions are viewed by private sector and government agencies as an opportunity to understand infection concentrations and the need for healthcare services and products. Moreover, the existence of pre-existing data infrastructure at the disposal of NIC and NDMA mean that such app-based solutions have the ability for large scale and efficient expansion in India.¹²¹ From a privacy perspective, since such apps probably are at their most efficient when they have continuous access to location data, which evoke reasonable apprehension of mass, real-time or dragnet surveillance.

Panoply of state government apps

38. But the notion of app deployment in pursuance of contact tracing is expanding at both central and state government levels.¹²² These mobile applications are being developed to track the spread of the virus and to also apprise people about threat vectors in their surroundings. Prominent ones mentioned at the central level which have come up across press reports include Aarogya Setu, Corona Kavach and Cowin-20. However, without any shred of privacy respecting standards state level applications for COVID-19 are particularly concerning.
39. In Goa, the state government has developed an app called *Test Yourself Goa*. It has been developed by the state's health department in conjunction with a healthtech company called Innovaccer.¹²³ Innovaccer has also tied up with the Puducherry Government to develop an analogous app called *Test Yourself*

¹²⁰ The National Disaster Management Authority (NDMA) has populated data it has access to from hospitals onto this repository which is subsequently accessed by private sector/third party developers.

¹²¹ Prasad Banerjee, *India taps location surveillance apps to keep virus in check*, Live Mint, March 2020, <https://www.livemint.com/technology/tech-news/india-turns-to-location-surveillance-to-contain-spread-of-covid-19-11585466140031.html>.

¹²² Abhik Sengupta, *Coronavirus Apps: Every App the Central Government and States Have Deployed to Track COVID-19*, NDTV, April 2020, <https://gadgets.ndtv.com/apps/features/central-state-governments-launch-coronavirus-mobile-app-list-2204286>.

¹²³ Aman Rawat, *#StartupVsCovid19: Innovaccer Aims To Curb Panic In Goa With Self-Diagnosis App*, Inc42, March 2020, <https://inc42.com/buzz/innovaccer-works-with-go-govt-for-coronavirus-self-diagnosis-app/>.

Puducherry.¹²⁴ These two apps allow users to fill up questionnaires which help in carrying out self-assessments, which helps advise on next steps based on symptoms without having to visit a healthcare facility.

40. In Tamil Nadu, the police has tied up with Pixxon AI Solutions to develop a COVID-19 quarantine monitoring application. Concerning from a privacy lens, is that the application allows both users and the government to monitor the live location of persons who are under home quarantine directives. The application also provides users with a self-assessment facility as well.¹²⁵
41. Karnataka of course has the much criticised *Quarantine Watch* application in which infected persons have been directed to enrol. These persons must send hourly selfies through the application which is geo-tagged and reviewed by a special review team. Karnataka's Geographic Information System Agency department has developed an app of its own called *Corona Watch*. The app reportedly requires access to a phone's location, media, storage, and network. The app informs users of the places a person confirmed to have the coronavirus, has visited in the days leading up to the diagnosis. It also shows users broad areas/localities in which residents have been asked to quarantine.¹²⁶
42. Then, in Maharashtra there is the *Mahakavach* application which has been developed by the Maharashtra State Innovation Society.. According to the developers of the application, it intends to fulfil two discrete roles namely: (1) improve contact tracing; and (2) track quarantine compliance.¹²⁷ According to one report the application is designed to provide details regarding public places¹²⁸ a diagnosed person has visited, travel history, and persons they may have come in

¹²⁴ Abhik Sengupta, *Coronavirus Apps: Every App the Central Government and States Have Deployed to Track COVID-19*, NDTV, April 2020, <https://gadgets.ndtv.com/apps/features/central-state-governments-launch-coronavirus-mobile-app-list-2204286>.

¹²⁵ Abhik Sengupta, *Coronavirus Apps: Every App the Central Government and States Have Deployed to Track COVID-19*, NDTV, April 2020, <https://gadgets.ndtv.com/apps/features/central-state-governments-launch-coronavirus-mobile-app-list-2204286>.

¹²⁶ Abhik Sengupta, *Coronavirus Apps: Every App the Central Government and States Have Deployed to Track COVID-19*, NDTV, April 2020, <https://gadgets.ndtv.com/apps/features/central-state-governments-launch-coronavirus-mobile-app-list-2204286>.

¹²⁷ Abhik Sengupta, *Coronavirus Apps: Every App the Central Government and States Have Deployed to Track COVID-19*, NDTV, April 2020, <https://gadgets.ndtv.com/apps/features/central-state-governments-launch-coronavirus-mobile-app-list-2204286>.

¹²⁸ Including hotels, restaurants, railway stations and religious destinations.

contact with. The app also integrates geo fencing (as per a predefined radius) and selfie attendance features to ensure people adhere to quarantine orders.¹²⁹

43. The reasons behind Mahakavach neatly summarises the primary purposes for which mobile applications are being developed in the context of coronavirus in India. Other state level apps are being developed in Gujarat and Himachal Pradesh as well.

Preventing mass surveillance through contact tracing

Assessing need, feasibility and risks

44. With the creation of such systems, come new risks of scope creep and new institutionalisation of mass surveillance. This becomes more important in India which lacks a comprehensive data protection law, outdated surveillance and interception laws, or any meaningful proposals for meaningful reform. Some experts like Sean McDonald¹³⁰ have discussed the issue of any deployment of contact tracing applications.¹³¹ He summarises the problem through the lens of his own experiences with tracking people's movements during humanitarian crises. First, he argues that although most of these apps are purported as 'contact tracing' technologies, they often devolve into systems of movement control and lockdown enforcement.
45. McDonald argues that while the technology helps, strong adherence to social distancing and lockdown measures is usually representative of the coercive power of a particular government. Using this he questions the tangible efficacy of contact tracing apps in augmenting national responses to the pandemic. He also argues that in such times the intrusive tracking and excessive health messaging can discourage citizens, since they feel bullied and stigmatised. More tangibly, the data collection can lead to leakages into the public domain, and in the current times leaves people prone to harassment.¹³²
46. McDonald further argues that in times of crisis, a lot of technology solutions with no demonstrable scientific value to the national response can be passed off as being in the public interest. He argues that it leads to poor deployment of scarce

¹²⁹ Alok Deshpande, *Mahakavach to ease contact tracing load*, The Hindu, April 2020, <https://www.thehindu.com/news/cities/mumbai/mahakavach-to-ease-contact-tracing-load/article31231782.ece>.

¹³⁰ CEO, Frontline SMS and Senior Fellow, Centre for International Governance Innovation.

¹³¹ Sean McDonald, *No, we don't need an app for this*, The New Humanitarian, March 2020, <https://www.thenewhumanitarian.org/opinion/2020/03/30/coronavirus-apps-technology>

¹³² Sean McDonald, *No, we don't need an app for this*, The New Humanitarian, March 2020, <https://www.thenewhumanitarian.org/opinion/2020/03/30/coronavirus-apps-technology>

public resources and also makes it difficult for crisis responders to discern between “snake oil” and quality technology products. These risks are exacerbated in technology markets since there are no adequate checks and balances in development phases which ensure quality.¹³³

47. McDonald unpacks the issue with leveraging smartphone based applications to determine hotspots and concomitant decisioning with respect to the allocation of medical/healthcare supplies. He relates this to his experiences with disaster relief efforts, where such systems inadvertently discriminate against regions which have fewer concentrations of smartphones. Specifically, it can lead to harmful outcomes for people from residing in economically weaker areas.
48. Finally, in countries public health systems are already creaking under the looming threat of capacity deficits. If such systems wrongly urge people to pre-emptively take tests then there is a risk that public health systems may be overwhelmed prematurely.¹³⁴ Without meaningful human rights considerations and appropriate safeguards there is a risk of further concentration in digital ecosystems. It may exacerbate the risks associated with the harvesting of personal data like health information, and also see the creation of new privacy invasive systems. Thus before these new systems are deployed at scale we must identify appropriate technological and computational models. These efforts must be to embed human rights and safeguards into the design of proposed systems itself.

Promising models for contact tracing applications

49. Globally, groups of volunteer technologists are framing coalitions trying to identify privacy-respecting deployments of contact tracing applications. One such coalition is called “stop-covid.tech”. Members of the group span Australia, US, UK and Switzerland. The objective of this group (like others), which collaborates through tools like Google Docs and Github is to build tools which can track the direction of the virus while protecting people’s privacy and without building permanent architectures of surveillance.¹³⁵
50. There of course remain disagreements on whether these contact tracing applications use Bluetooth, a cellular network or GPS coordinates. One media report which surveyed a series of these projects found certain commonalities:

¹³³ This is in contrast to vaccine development where even an expedited response will still need to conform to various regulatory and safety protocols

¹³⁴ Sean McDonald, No, we don’t need an app for this, The New Humanitarian, March 2020, <https://www.thenewhumanitarian.org/opinion/2020/03/30/coronavirus-apps-technology>

¹³⁵ David Ingram and Jacob Ward, Behind the global efforts to make a privacy-first coronavirus tracking app, NBC, April 2020, <https://www.nbcnews.com/tech/tech-news/behind-global-efforts-make-privacy-first-coronavirus-tracking-app-n1177871>

- a. The usage of these applications should be voluntary (unlike Israel and Chinese surveillance operations);
 - b. All data should always be stored locally on people's devices;
 - c. This data must be encrypted;
 - d. No Government can access it at a later point
51. As the leader of an app development initiative in Switzerland puts it, their sole goal is to ensure that nothing is centralised in a server. These initiatives take inspiration from systems like Apple's *Find My iPhone* which uses anonymisation, encryption and Bluetooth.¹³⁶ A notable initiative is being pioneered by the Massachusetts Institute of Technology (MIT) called *Safe Paths*. The leaders of this initiative would like to work toward building human facing tools, which can tell people if they are in a good situation or not.¹³⁷ Such initiatives aim to improve deployments in countries like Singapore. Some machine learning practitioners and critics suggest that Singapore does not adhere to principles of data minimisation.
52. As Ryan Calo has argued there also exists the risk that even the best intentioned technological solutions with impeccable design is susceptible to manipulation and panic. Instead of improving the situation, such technologies run the risk of becoming a hurdle to the fight against the pandemic.¹³⁸ As such while the answer is complex, the problem statement which all stakeholders are trying to solve is simple to articulate.
53. On March 23, 2020 a group of technologists shared an open letter to the digital transformation unit of UK's National Health Service (NHSX) on the ethical deployment of contact tracing systems.¹³⁹ The letter highlighted that missteps

¹³⁶ David Ingram and Jacob Ward, *Behind the global efforts to make a privacy-first coronavirus tracking app*, NBC, April 2020, <https://www.nbcnews.com/tech/tech-news/behind-global-efforts-make-privacy-first-coronavirus-tracking-app-n1177871>

¹³⁷ David Ingram and Jacob Ward, *Behind the global efforts to make a privacy-first coronavirus tracking app*, NBC, April 2020, <https://www.nbcnews.com/tech/tech-news/behind-global-efforts-make-privacy-first-coronavirus-tracking-app-n1177871>

¹³⁸ David Ingram and Jacob Ward, *Behind the global efforts to make a privacy-first coronavirus tracking app*, NBC, April 2020, <https://www.nbcnews.com/tech/tech-news/behind-global-efforts-make-privacy-first-coronavirus-tracking-app-n1177871>

¹³⁹ Joint Letter, *Open Letter: Contact Tacking and NHSX*, Medium, March 2020, <https://medium.com/@rachelcoldicutt/open-letter-contract-tracking-and-nhsx-e503325b2703>

during the ongoing public health crisis may have long term ramifications as well. Pillars of ethical development of these systems include:

- a. Working in the open with publication of machine readable data and models
 - b. Mandating rights and privacy impact assessments, for all new technologies introduced during this public health crisis
54. Aside from protecting human rights, they suggest that government measures must be proportionate and work within the rule of law.¹⁴⁰ Indeed, this appears to echo the views of numerous technologists and civil rights advocates including Professor Hu Yong who has written a widely cited article on individual privacy during a public health crisis.¹⁴¹
55. In this light governments should not deploy untested new technologies without ethical safeguards like good governance, transparency and a willingness to course correct. They urge governments to not use emergency powers under general statutes to track and detain people without appropriate line of sight and transparency.¹⁴² Further, they highlight the limitations of contact tracing with respect to inaccuracy and how it disadvantages people without smartphones-- which in India is more than two thirds of its 1.3 billion population.

Design and rights imperatives for contact tracing applications

56. When it comes to the general development of applications, websites and platforms, governments would do well to avoid falling into the traps of “techno-solutionism” and investing in large scale surveillance systems.¹⁴³ Novel technological solutions must tread lightly since it may lead to operating outside legal systems, the creation of new and weaker legal systems, and the potential harvesting of personal data in centralised servers. Moreover, investments into new expensive systems of surveillance, will make it difficult to undo at a later

¹⁴⁰ Joint Letter, *Open Letter: Contact Tacking and NHSX*, Medium, March 2020, <https://medium.com/@rachelcoldicutt/open-letter-contract-tracking-and-nhsx-e503325b2703>

¹⁴¹ Hu Yong, *The Public Interest and Personal Privacy in a Time of Crisis (Part II)*, As translated in the ChinAI Newsletter, March 2020, <https://mp.weixin.qq.com/s/2KRGP2ErKIQ9XF98asy8-w?fbclid=IwAR24LIWvXNkxjR69sKsduoPp9cVwSCsMthAYCXXdUoqC3mooPvLWZYGIk4>.

¹⁴² Joint Letter, *Open Letter: Contact Tacking and NHSX*, Medium, March 2020, <https://medium.com/@rachelcoldicutt/open-letter-contract-tracking-and-nhsx-e503325b270>.

¹⁴³ *Recommendations on Privacy and Data Protection in the Fight Against COVID-19*, Access Now, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>.

stage¹⁴⁴. Therefore, from the offing there should be a decision to avoid building large scale machinery to this effect.

57. The extraordinariness of the moment with this public health crisis should not lead to the creation of extraordinary systems of dragnet surveillance. Post September 11, 2001, America and in fact countries across the world saw the advance of extraordinary surveillance capabilities. This was done through tactics of evangelising the need for surveillance in the fight against terrorism. This has of course been revealed to the general public with devastating effect through the Snowden revelations.

58. To avoid, allowing this pandemic to have a similar long term effect and for the creation of invasive over the skin and under the skin surveillance¹⁴⁵, advocates push for two key principles¹⁴⁶:

- a. Strict limits (in terms of collection and duration)every step of the way; and
- b. Comprehensive evidence-based justifications every step of the way.

59. More specifically, experts from groups like the Electronic Frontier Foundation and the American Civil Liberties Union (ACLU) suggest that data-based responses to this pandemic should be driven by healthcare officials, healthcare experts and experts in the field of epidemiology. The involvement of the security or law enforcement community may carry its own set of risks and conflicts of interest. Additionally, global experts indicate that this data should be walled off in a manner where there is no risk that it merges or is combined with other databases. This data cannot be used for other purposes like to imprison people, or for immigration, public benefit delivery or tax collection.¹⁴⁷

60. To put it concretely, data driven contact tracing may help a country like India move away from a country-wide lockdown. It may even be a useful tool in getting people back into their jobs while saving people's lives during this public health crisis. However, any contact tracing app developer must answer/address the following aspects¹⁴⁸:

¹⁴⁴ Leading to the creation of data dragnets

¹⁴⁵ Yuval Noah Harari, *The World After Coronavirus*, Financial Times, March 2020, <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75>.

¹⁴⁶ Sam Biddle, *Privacy Experts Say Responsible Coronavirus Surveillance is Possible*, The Intercept, April 2020, <https://theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/>.

¹⁴⁷ Sam Biddle, *Privacy Experts Say Responsible Coronavirus Surveillance is Possible*, The Intercept, April 2020, <https://theintercept.com/2020/04/02/coronavirus-covid-19-surveillance-privacy/>.

¹⁴⁸ Yves-Alexandre de Montjoye and others, *Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask*, Computation Privacy Group, April 2020,

Source: Privacy Computational Group Blog Post ([Link](#))

1. Appreciate that any data from location information, to proximity confirmations, to health status, to whether they have been placed in isolation is sensitive personal information.	2. Privacy by design in contact tracing is more than just assurances that phone numbers are not recorded, all data is encrypted, pseudonymisation is deployed or that the use of the app is “voluntary” and based on consent. Most of these protections have known techniques of circumvention.
3. What is the protocol or technique deployed to limit a public authority’s access to personal data?	4. How are people’s anonymity/identity protected? Specifically, what are the special measures put in place to ensure people cannot be reidentified by external parties and/or the government.
5. Technologists argue that the goal of a contact tracing application is to empower users with the knowledge that THEY have been in contact with an infected person. The authority should not be given direct information about these people’s identities.	6. Digital contact tracing should warn people without revealing who may have put them at risk of getting infected. Users should not be able to use the system to deduce who may have infected them.
7. Your system should not allow users to learn about other people’s movement trajectories, networks or other personal information.	8. Consistent digital identifiers leave people vulnerable to attacks from malicious actors. Systems which keep updating device identifiers with regularity remain safer from attacks.
9. What are the special efforts made to protect the personal details of infected persons (typically the most vulnerable in the crisis)?	10. Large scale contact tracing systems carry very sensitive connotations for users. Therefore, governments must operate them with transparency. This allows for external actors to audit the government’s claims and facilitates healthy scrutiny. Publication of source code, and encouraging security research to reverse engineer the systems are important to test for robustness.

<https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/>.

6. Incentive structures for adoption

1. The effectiveness of these apps, of course, depend on how many people install it. A recent study published on Oxford confirms this. It says that if enough people use contact tracing technologies, then it will help with epidemic control.¹⁴⁹ This may afford authorities the space to relax social distancing norms and restart normalcy in economic activities. However, this is where things get complicated.
2. The risks to individual privacy associated with digital contact tracing, location tracking and the use of health data have been discussed in great detail throughout this report. Other risks which come with adoption of such systems may be summarised through the lens of:
 - a. Information Security: While many apps do not upload data automatically, on-device logs are also susceptible to being read by malware or those with physical access to the device.
 - b. Agency: The patient has control over the information he or she reveals during a physical contact tracing interview. This is typically not the case whilst using these apps.
 - c. Convenience: Primarily battery life and may lead to devices performing sub-optimally, or shutting down prematurely-- rendering the apps irrelevant.
3. Most people may consider these costs to be minor compared to the benefits; some may even think that *having these concerns* should be punishable, in these frightening times. However, if there are technical measures to bake privacy by design then such concerns would be sufficiently addressed. We must impress that the technical protections and safeguards may further require clear legal guidance on the collection, use and limitation of personal data that is used through such applications.

Sensitivity to individual autonomy furthers user trust

4. The Government and developers must be sensitive to the different people whose rights and interests are impacted by contact tracing technologies. Without trust many people will stay away from installing these applications which, if “voluntary” by design, will lead to its ultimate failure. Even if it succeeds, poor design may lead to harmful consequences for people’s rights. Critically, the European Data Protection Supervisor has expressed a concern which holds resonance in India as well. The EDPS has rightfully pointed out that a multiplicity of apps, with little consistency in standards ultimately lead to a race to the bottom, where privacy may be irreparably harmed.

¹⁴⁹ Luca Ferretti and Others, *Quantifying SARS-COV-2 transmission suggests epidemic control with digital contact tracing*, Science.org, March 2020, <https://science.sciencemag.org/content/early/2020/03/30/science.abb6936>

5. The different stakeholders who are impacted by contact tracing technologies are not just the app's users but even those in their social and geographical vicinity. Broadly we may categorise parties impacted by these technologies into four broad buckets¹⁵⁰:
 - a. People who have been infected with the novel SARS-COV-2 disease
 - b. Depending on the technology system deployed, people who have, or may have, come into contact with an infected person.
 - c. In a post-lockdown world, establishments visited by infected persons during the period of contagion (as determined by the application)
 - d. People who are associates of individuals who are confirmed to have been infected by the coronavirus.
6. For a system to be successful, these different groups of parties must have the requisite trust to safely use the application. The value proposition of the application must be compelling enough for people to join without coercion. Additionally, the churn should remain low and people should believe there is value in using it in a continual fashion during the course of the pandemic. App developers know this, and have used a variety of strategies to combat it:
 - a. Design the app and process to minimize these costs while retaining the benefits.
 - b. Appeal to social responsibility.
 - c. Cover up or obfuscate what the app does.

Case study: Iran

7. Trust is central to large scale and sustained adoption. A lack of public trust in the government would mean control measures will not work. The other option i.e. state coercion is not compliant with rule of law and constitutional imperatives. Existing legal systems in India do not allow for legitimate state intrusions into people's personal and sensitive personal information. This is because India still lacks a surveillance framework and a Personal Data Protection framework which is aligned with the thresholds which have been laid down by its Supreme Court in *KS Puttaswamy v Union of India*¹⁵¹.
8. We may draw on learnings from Iran's experience with its government developed AC-19 application. Its Government published this application to help people with self-diagnosis and alleviate growing pressures on Iranian hospitals. The application was available through a website and other third party app stores.

¹⁵⁰ Ramesh Raskar and Others, *Apps Gone Wrong: Maintaining Personal Privacy in an Epidemic*, Private Kit: MIT | Whitepaper, March 2020, <https://arxiv.org/pdf/2003.08567.pdf>.

¹⁵¹ See earlier sections of this paper.

However, in March 2020 Privacy International's COVID-19 surveillance tracker confirmed that Google had removed the application from its Play Store.¹⁵²

9. Iranian citizens were concerned that the application was being deployed by the Government as spyware. These concerns were exacerbated by mass messaging by the government urging people to download and install the application. Further, the terms and conditions and accompanying policies did not disclose the purpose for which the application was collecting real-time location details.
10. Local reports even revealed that the app was developed by a technology vendor which has previously been linked with helping Iranian intelligence agencies develop applications which clone versions of Telegram, widely believed to be spyware deployed on behalf of the state.¹⁵³ In addition, the self-diagnosis application was used to build large-scale location insights on millions of Iranians, which suggested contravention with established principles of purpose limitation.¹⁵⁴
11. It may be surmised that this initiative of the Iranian Government suffered from a trust deficit. This is owing to: (a) the public's perception of the technology vendor which developed the application; (b) the purposeless collection of people's location data; and (c) the lack of transparency with respect to core details pertaining to the application.

7. Analysis of contact tracing applications developed by Singapore, MIT and India

1. For completeness and objectivity this paper has also studied three existing models of contact tracing applications. The first is Singapore's much-discussed *TraceTogether* application which has been built on the underlying *BlueTrace* protocol. The second is MIT's open-source *Private Kit: Safe Paths* project. The third is the Central Government of India's official contract tracing application

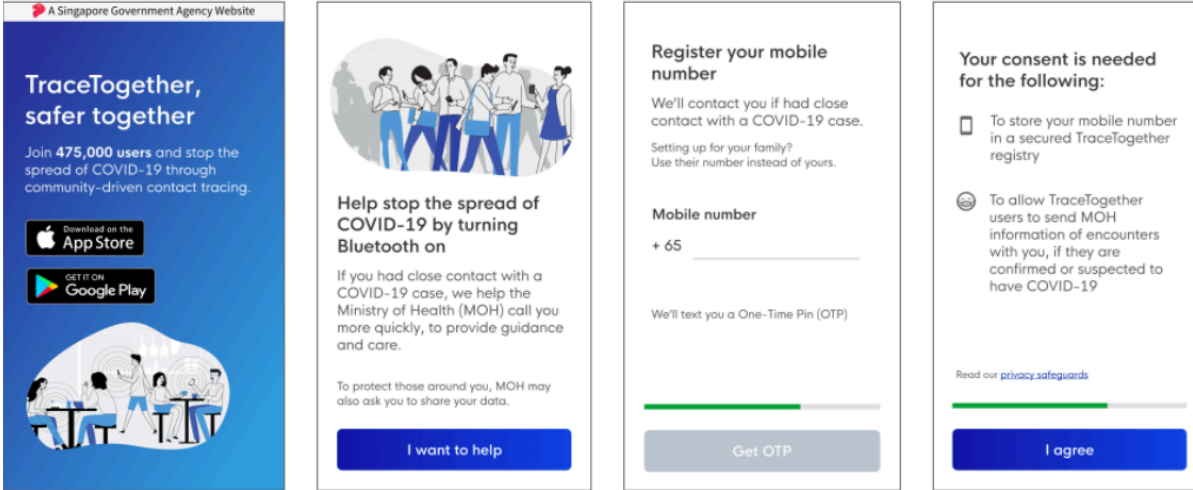
¹⁵² Iran: Google withdraws Iranian COVID-19 self-diagnosis app, Privacy International, March 2020, <https://docs.google.com/document/d/1nDoPzygQyTetEguOlzula5O9y5f3f5YJDsA2Pd99O6U/edit#>.

¹⁵³ Catalin Cimpanu, *Spying concerns raised over Iran's official COVID-19 detection app*, March 2020, <https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/>.

¹⁵⁴ David Gilbert, *Iran launched an app that claimed to diagnose coronavirus. Instead, it collected location data on millions of people*, VICE, March 2020, https://www.vice.com/en_in/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people.

which is called *Aarogya Setu*. As of writing, *Aarogya Setu* has already been reportedly downloaded by the public more than 21 million¹⁵⁵ times.

Case study 1: TraceTogether (Singapore)



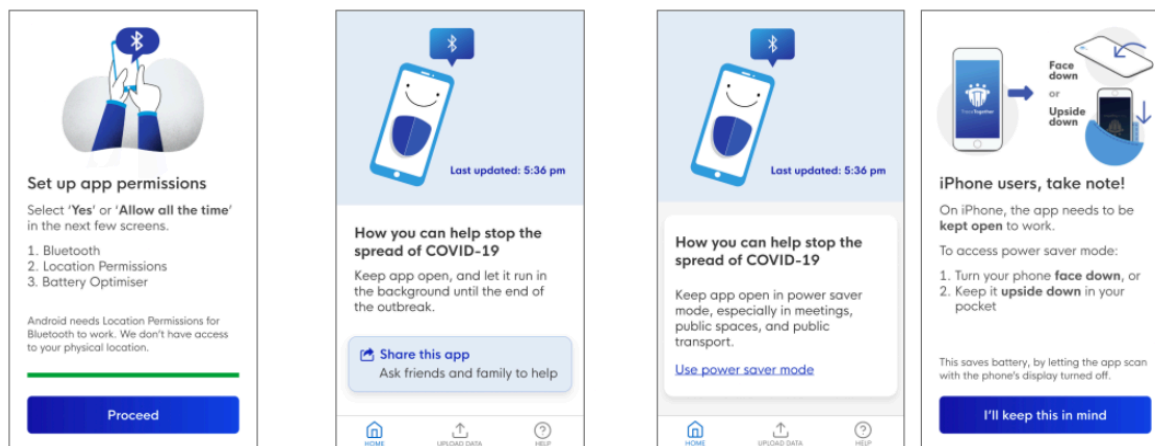
1. Tap on App Store or Google Play to download
2. Launch app and go through the onboarding flow
3. Enter your mobile number and One-Time Pin
4. Give consent

2. The application is available for download at Apple's App Store and Google's Play Store, and is only compatible with Bluetooth equipped smartphones. Users do not need to be connected to the internet to use the application. Its primary purpose is to alert users if they have had close contact with a person diagnosed with COVID-19. The application has been built on an open source protocol called *BlueTrace protocol*, developed by Singapore's Health Ministry and its Government Technology Agency.
3. The source code for the android and iOS applications, and its cloud function is available on GitHub.¹⁵⁶ Stakeholders may use it via the GNU General Public License Version 3¹⁵⁷. The protocol is intended to be applied to both mobile apps and wearable devices. A long term aspiration of this project is to make this protocol an interoperable standard for future applications across the world.

¹⁵⁵ Karishma Mehrotra, *Behind Aarogya Setu app push: 'At least 50% people must download for impact'*, Indian Express, April 2020, <https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/>.

¹⁵⁶ <https://github.com/OpenTrace-Community>.

¹⁵⁷ GNU General Public License, Version 3, 29 June 2007, <https://www.gnu.org/licenses/gpl-3.0.en.html>.



5. Set up app permissions

[Android phones](#)

6. Set up completed!
Keep the app open in the background until the end of the outbreak.

[iOS / iPhones](#)

6. Set up completed!
For iPhones, the app works best in the foreground. We recommend you to keep the app open in meetings and crowded places.

4. On first launch, users register using mobile number verification, and a unique ID is generated for the user. The government maintains a database mapping phone numbers to unique IDs. These IDs are temporary in nature and are periodically changed to protect users against information security threats posed by malicious actors.

Permissions sought : user consent is present but not absolute

5. The collection and logging of encounters between devices is done in a decentralised P2P manner. When two phones with the app come within Bluetooth range, they share their IDs with each other; an encrypted log of these exchanges is stored on each phone. The application determines what constitutes “close contact” based on standards and thresholds set by the Ministry of Health’s contact tracers. According to these standards the application sends curated advice to users.
6. The website of the application advises users that the application should be running with full permissions at all times during the course of the COVID-19 outbreak. Users nonetheless have the option to switch off bluetooth access or delete the application.
7. Information relating to proximity and duration is stored on a user’s phone, after which data is deleted on a rolling basis every 21 days. Also should a user delete the application from their phone, all locally stored data is deleted. The app’s official website asserts that it does not collect the location data of users. While it does require permissions for the device’s location for Android devices only, the

website maintains that this permission is sought solely to be allowed access to the mobile's Bluetooth¹⁵⁸.

8. Should an individual contract the disease, Singapore's Health Ministry will work with them in contact tracing and determine who they have been in close contact with in a 14 day period. In this context, users of the *TraceTogether* application can grant access to their Bluetooth contact/proximity information with the Ministry of Health, to support faster detection of transmission. We must highlight that while this appears positive, as discussed earlier in this paper, people in Singapore can be prosecuted under its Infectious Diseases Act (Act No. 21 of 1976) should they impede the Government's contact tracing efforts.
9. Notably, the health ministry has mentioned that contact tracing applications cannot be a substitute for human contact tracing initiatives, and can only serve as an alternative. Human involvement from such practices cannot be removed. If an individual deletes their application, they will not be able to share their stored logs with contact tracers.
10. It appears that the *TraceTogether* app does not function efficiently when in the background on phones which use iOS. This can be punishing on the battery lives of such devices, makes it difficult to use the app in conjunction with other apps, etc. To overcome this they have built a "Power Saver" mode for iOS users. Android users have been instructed to keep the app open for the duration of the pandemic. Such requirements may even have long term effects on the battery reliability of certain mobile devices.

Privacy and security safeguards : do users have full control?

11. The *TraceTogether* Privacy Statement¹⁵⁹ asserts that efforts are made to ensure users have control over their personal information. While most information is stored locally, the statement does state that the Government collects and stores people's mobile number and a permanent anonymised user ID in a centralised Government server.
12. Contact confirmations are only administered through Bluetooth. The Privacy Statement assures users that the application does not collect information pertaining to GPS locations or WiFi networks. It states that when establishing contact with other phones in the area, both phones exchange a Temporary ID which is essentially an encrypted communication of each device's user ID. Notably, the private key to these temporary IDs are held by the Ministry of Health, who is the only authority with the power to decrypt these logs.

¹⁵⁸ Owing to rules set with respect to permissions by Google's Play Store.

¹⁵⁹ Government of Singapore, Ministry of Health and GovTech, *TraceTogether Privacy Safeguards*, <https://www.tracetogogether.gov.sg/common/privacystatement>.

Moreover, even if decrypted, the obfuscated user ID by itself is unlikely to reveal a person's identity, to an external actor.

13. All data about phones in a particular vicinity are stored on phones. If a user of this application does get infected with the coronavirus, then they have the option to share their *TraceTogether* logs with Singapore's Ministry of Health. Temporary IDs which are shared with other devices when contact is established, are updated by the application periodically. It is claimed that such periodic updation of the temporary ID which is shared with other devices, means there is no persistent identifier of a device. This makes it impossible for third parties to track you using the application. The time period between updations of temporary identifiers is not specified.
14. People are also granted the ability to revoke consent. They can share an email request along with their mobile number used to sign up with the application. This means all data stored in the centralised database will be deleted. The Privacy Statement also asserts a strict purpose limitation. All data which is collected through the *TraceTogether* app, will solely be used for contact tracing/epidemiological purposes. The application that once the need for contact tracing ceases, they will prompt users to disable the tracking function. Anonymised data from devices and the app itself (device model, app version) is collected for technical analysis and updates¹⁶⁰.

State-coercion to access contact tracing information

15. FAQs on the *TraceTogether* application clearly reiterate the position of Singapore's Infectious Diseases Act, where punishment for contravention includes possible imprisonment up to 6 months. Specifically, people are required by law to strictly assist the Ministry of Health's contact tracing team, tracking the spread of the disease.
16. This includes location timelines and device level logs. The FAQs also suggest that users of the application who have tested positive for the novel virus may also have to share logs and location timelines which may be shared with other applications like Google Maps.¹⁶¹ This certainly may undercut ideas of user autonomy and control over personal data.

¹⁶⁰ *TraceTogether* uses Google Firebase for analytics.

¹⁶¹ *Trace Together FAQs, Permissions and Privacy, Privacy and Data, Can I say no to uploading my TraceTogether data when contacted by the Ministry of Health?*, March 2020, <https://tracetogogether.zendesk.com/hc/en-sg/articles/360044860414-Can-I-say-no-to-uploading-my-TraceTogether-data-when-contacted-by-the-Ministry-of-Health->.

So how do users audit these representations?

17. Since *TraceTogether* is built using the Government of Singapore's *BlueTrace* protocol, stakeholders (primarily technologists) can audit the code. However, there is no individualised mechanism or avenue for judicial review or remedy for users to hold the application legally accountable.

Case Study 2: PrivateKit : SafePaths (MIT)

18. A major challenge for Bluetooth based smartphone applications is exclusion. In a country with more than 1.3 billion people, only around 400 million people would have access to smartphones. This means more than two thirds of the population do not have access to devices over which such solutions are being developed.
19. For a broader user case and greater inclusivity researchers at universities like MIT's *Safe Paths* team alternatives are developing tracing solutions based on GPS location coordinates. As the evidence of how the coronavirus spreads evolves the use of these alternatives are important to consider. For instance, there is growing evidence that the disease spreads via surfaces even a long period after first exposure. Some technologists therefore believe it may become important to map where people went rather than who they were in contact with. The privacy risks with such an approach obviously grow.
20. In such a paradigm, technologists and governments may argue that mapping people's movements and trajectories becomes an essential facet of reducing transmission. Any decision to go down this path must be accompanied with supporting evidence, justifications and inputs from healthcare and disease experts. MIT's *Safe Paths* team is developing a GPS-based solution which may be used by international organisations like WHO. However, since GPS data is harder to anonymise/obfuscate, the team is exploring technical solutions along the lines of stronger encryption.¹⁶²

Underlying principles and assumptions of the project

21. The *Safe Paths* project was conceptualised in a concept note which seeks to answer a simple question: how society can restart its economy, whilst reducing the risk of widespread infection. It refers to the need for creating a "safe worker" workforce, where people have been "certified" as carrying antibodies which means they have built a degree of immunity against the coronavirus. There is already considerable dialogue around the idea of "immunity passports" in the context of COVID-19.

¹⁶² Hannah Murphy, *US and Europe race to develop 'contact tracing' apps*, Financial Times, April 2020, <https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95>

22. Conversely, it also discusses the value of “certifying” if people have tested negative for the virus. Such “certification” may even be applicable to public spaces, shops, establishments, etc. At an aggregate level the concept note states that such data help with contact tracing and early detection. However it states that the creation of “safe workforces” may justify crude government tactics. The use of large data methods evoke concerns of Orwellian outcomes. To avoid this there is an onus on democratic governments to create sophisticated computing techniques¹⁶³ which can preserve people’s privacy and control over their personal data.¹⁶⁴
23. In a subsequent whitepaper on personal privacy of such apps, it is stated that such apps can support containment of the coronavirus.¹⁶⁵ Towards this key steps include:
- a. Rapid identification of infected persons;
 - b. Quarantine of infected persons;
 - c. Establishing persons with whom close contact was made in the run up to the diagnosis; and
 - d. Decontamination of visited locations.
24. Towards this it discusses the value of creating timestamped logs of people’s location trails tracked through GPS. When the location trails of an infected person are compared with other people’s location trails, a chain of infection (through close proximity tracking) is easier to detect. However, the trick is balancing this imperative whilst preserving people’s fundamental freedoms, individual privacy and preventing mass surveillance. Therefore, they have sought to build a citizen-centric, privacy-first contact tracing application which is open-source, secure and decentralised.

Design features : towards a privacy-first app

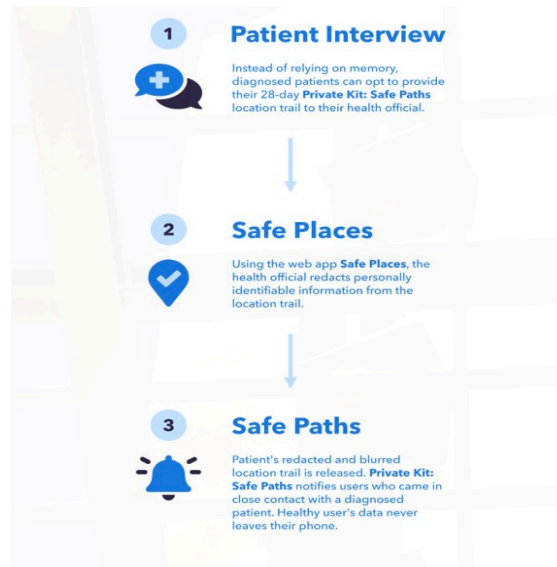
25. In the first iteration of the *Private Kit: Safe Path* application users are allowed to log their personal location trails on their devices. Upon diagnosis, infected persons can share their location trails with health officials. What happens if a user who has been infected refuses to share such information with officials, remains to be seen.

¹⁶³ E.g. (a) Secure Multiparty Computation and (b) “risk maps” aggregated from anonymized data and appropriately sanitized using differential privacy methods (such as employed by the U.S. Census Office).

¹⁶⁴ MIT Connection Science, *Restarting the Economy and Avoiding Big Brother: We need to know who is immune and employ them in the front line*, http://connection.mit.edu/sites/default/files/publication-pdfs/Restarting%20the%20Economy_0.pdf.

¹⁶⁵ Ramesh Raskar and Others, *Apps Gone Wrong: Maintaining Personal Privacy in an Epidemic*, Private Kit: MIT | Whitepaper, March 2020, <https://arxiv.org/pdf/2003.08567.pdf>.

26. The second iteration of the application also equips users with notifications if they have established contact with a diagnosed carrier. Here the application affords Governments the discretionary option (through an application interface) to redact location trails. Such a feature allows governments to undertake contact tracing while affording privacy to disease carriers. The feature is also meant to offer reputational protections for establishments which are visited by disease carriers. However, it still raises the concern here that government officials do receive access to people's personal and sensitive personal information.



27. The third iteration, allows for a more federated model. In it diagnosed carriers are allowed to share privacy-protected location trails as push notifications to users who would have been in close proximity to the carrier. This iteration does not allow for a third party (like government) to facilitate dissemination of notifications. The application does not collect any user information on an external server. This feature is meant to stave off government surveillance. The idea is although GPS location trails are logged, they are not accessible by third parties and can only be stored in a time restricted manner in people's devices. Any sharing of these trails or any other personal data to an external cloud can only happen with user consent.

Specifics of the application and its privacy practices

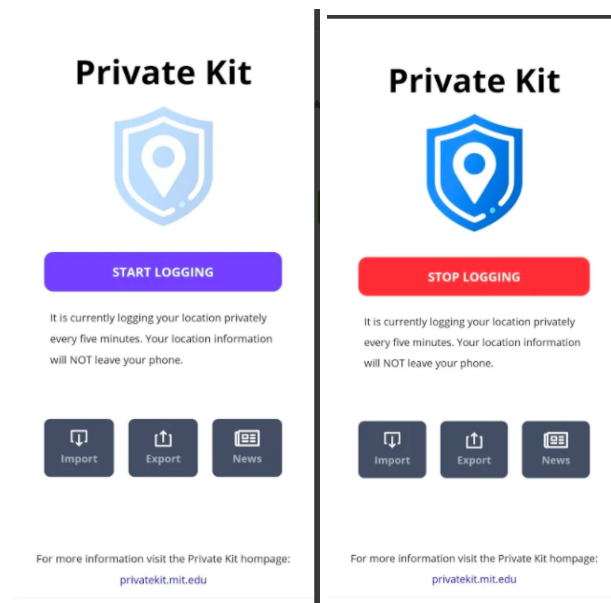
28. For public auditability the application is built on an open source protocol which is accessible on Github.¹⁶⁶ Prototype versions of the *Private Kit: Safe Paths* app are available for download on Android and iOS.¹⁶⁷ Its listing on Apple claims that it is a 'privacy-first' application which allows users to log their GPS trails on their

¹⁶⁶ Github repository of COVID Safe Paths protocol which is based on Private Kit, <https://github.com/tripleblindmarket/covid-safe-paths>.

¹⁶⁷ Private Kit, Welcome to Private Kit, <http://privatekit.mit.edu/>,

phone. The data is designed to be stored only on the concerned device and cannot be accessed outside of the device (even by the developer).

29. The user has the autonomy to manually export the logs to an external server. For instance, to share location trails with the researcher on an external server the user must authenticate approval via a QR Code. The location logs generated through the app can only be accessed through the user's device. To work, the app needs access to the user's location and motion tracking sensors. The trail generator is designed to track a user's device every 5 minutes, and stores logs for 28 days.



30. What may require some discussion vis-a-vis purpose limitation, is the lens through which the application is being developed. Contact tracing has been mentioned as the primary purpose of the *Private Kit: Safe Paths* project. However, its website envisions leveraging collected datasets for a range of other purposes like study of people's well being, refugee migration and community traffic analysis. Thus, the incentives of the project may not be geared towards purpose limitation and user deletion of the application (unlike Singapore's *TraceTogether* Initiative).
31. Another challenge is that the application does not have an application specific privacy policy for the specific project. This means there are no project specific principles of data minimisation, purpose limitation to the particular project and so on. The applicable privacy policy is the one which is a part of the University's general policy and procedures.¹⁶⁸ Moreover, the Privacy Policy is not clear as to

¹⁶⁸ MIT Policies, Policies and Procedures, 11.2 Privacy of Personal Information, <https://policies.mit.edu/policies-procedures/110-privacy-and-disclosure-personal-information/112-privacy-personal>.

how users can hold the Project accountable with respect to its interactions with external researchers, and Government authorities. There are no limitations placed with how this data may be shared with law enforcement authorities for instance. Nor is the Privacy Policy clear as to how user consent will be meaningful should it conflict with Government interests or requests.

Auditability of the application

32. There is no mechanism for remedy mentioned in the Privacy Policy. Nor is there a reference to any dispute settlement mechanism. Pertinently, there is no established mechanism through which people can enforce data deletion requests, revoke consent or check if requests to delete individualised data logs have in fact been complied with.

Case study 3: Aarogya Setu (Government of India)

Background to the application

33. Perhaps inspired by Singapore and China's usage (discussed earlier in this paper) of technologies for containment, multiple reports emerged that NITI Aayog, India's central policymaking arm, and MeitY were separately developing contact tracing applications to contain the novel coronavirus. A beta version of a contact tracing app called *Corona Kavach* (roughly translated from Hindi to "Shield of Corona") was temporarily available for download by Android devices via Google's Play Store.
34. This application was developed by the National e-Governance Division (NeGD) at MeitY, and was released in association with the Ministry of Health and Family Welfare (MoHFW). It was abruptly removed from Play Store and is no longer available for download. The removal of *Corona Kavach* was swiftly followed by a soft launch of an application called *Aarogya Setu* which translates from Sanskrit to 'a bridge of health'.
35. Considering the abrupt change the Government took the liberty to notify citizens to delete *Corona Kavach* and download the new *Aarogya Setu* application. The new application is available for download on both Google's Play Store and Apple's App Store.¹⁶⁹ It is curious that India is choosing to go down this route since it will exclude non-smartphone users, who constitute more than two thirds the country's population, from availing these benefits. What is more interesting is that even people in the initial development of the application have stated that at least 50 percent of the population must download the app for it to

¹⁶⁹ Saurabh Singh, *Govt discontinues Corona Kavach, Aarogya Setu is now India's go-to COVID-19 tracking app*, April 2020, <https://www.financialexpress.com/industry/technology/govt-discontinues-corona-kavach-aarogya-setu-is-now-indias-go-to-covid-19-tracking-app/1919378/>

be an effective solution.¹⁷⁰ Considering India does not have that many smartphones, would it mean the app is already set up to fail?

36. Initial reports suggested that the application uses a combination of both Bluetooth and GPS location. In addition the application has access to the Government of India's database in which it stores information relating to known cases.¹⁷¹ Unlike Singapore and MIT, India's contact tracing project lacks transparency. For example, there is no adjunct manifesto or website which details the project and the purposes thereof. Therefore, our analysis of this application is based on press reports, a quick glance through the application's front end features, its Terms of Service and Privacy Policy.

A systemic lack of auditability and transparency

37. Upon launch, the primary purpose of the application was positioned as notifying users of the application if they are at risk of contracting the novel coronavirus.¹⁷² However, reports indicate that the scope and purpose of the application may be much broader. For instance, the Government has reportedly set up a committee to actively monitor data which is captured by the Aarogya Setu application. The Committee is also entrusted with the mandate of using insights from this application and other technologies like those collected by drone vendors¹⁷³, in determining if India should relax lockdown conditions.¹⁷⁴ Reports even suggest that the application may be used to initiate geo fencing mechanisms.
38. Unfortunately, such practices have been popular in Asian countries with notably poor track records when it comes to civil and political rights. Reportedly, the Government may use the application to track violations of quarantine orders.

¹⁷⁰ Karishma Mehrotra, *Behind Aarogya Setu app push: 'At least 50% people must download for impact'*, Indian Express, April 2020, <https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/>.

¹⁷¹ Saurabh Singh, *Govt discontinues Corona Kavach, Aarogya Setu is now India's go-to COVID-19 tracking app*, April 2020, <https://www.financialexpress.com/industry/technology/govt-discontinues-corona-kavach-aarogya-setu-is-now-indias-go-to-covid-19-tracking-app/1919378/>.

¹⁷² Aarogya Setu Coronavirus tracking app now available on Android, iOS: Here's how to download and use, India Today, April 2020, <https://www.indiatvnews.com/technology/news-aarogya-setu-coronavirus-tracking-app-how-to-use-it-603851>.

¹⁷³ Supplied by six unnamed technology vendors.

¹⁷⁴ Vasudha Venugopal, *Aarogya Setu, drone data to play part in lockdown exit strategy*, Economic Times, April 2020, <https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/aarogya-setu-drone-data-to-play-part-in-lockdown-exit-strategy/articleshow/75040648.cms?from=mdr>.

The platform has been designed in a manner where datasets can be collated in centralised servers if the need arises.

39. There is no formal notification in the public domain which acknowledges the constitution of this committee. However, reports suggested that it may be headed by Mr Amitabh Kant i.e. the Chairperson of NITI Aayog. Other government representatives include officials from the Ministry of External Affairs; Ministry of Home Affairs (including the National Disaster Management Authority); Department of Telecommunications; and MeitY.
40. The absence of healthcare officials in a committee like this which is accessing data from the *Aarogya Setu* application is particularly concerning. It raises concerns of a surveillance system being set up. The Committee cited here is reportedly mulling recommendations to expand the Government's powers in using technological tools-- like the *Aarogya Setu* application. In fact it has reportedly already made a specific recommendation to extend and expand the scope of the application post the lockdown.¹⁷⁵

Uncoding the underlying assumptions of Aarogya Setu

41. *Aarogya Setu*'s listing on Google's Play Store and Apple's iOS confirm that its primary developer is India's National Informatics Centre (NIC) which is under MeitY. There is no reference to whether the application was developed in conjunction with non-government stakeholders/vendors. The accompanying description of the application remains vague and states that the app has been designed to, "... connect health services with people of India in our combined fight against COVID-19."¹⁷⁶
42. What is revealing that it is meant to allow the MoHFW to proactively reach and inform users regarding risks, best practices and advisories. This appears to suggest that the application is meant to be an all purpose portal of which contact tracing is but one element. Its compatibility with purpose limitation and data minimisation principles seems difficult to reconcile.
43. The application is designed in a manner where a user's risk level of exposure to COVID-19 is represented according to a colour coded warning system. At this stage, given the lack of an accompanying website or blog post or manifesto, it is prudent to unpack the *Aarogya Setu* app's Terms of Service and its Privacy Policy.

¹⁷⁵ Vasudha Venugopal, *Aarogya Setu, drone data to play part in lockdown exit strategy*, Economic Times, April 2020, <https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/aarogya-setu-drone-data-to-play-part-in-lockdown-exit-strategy/articleshow/75040648.cms?from=mdr>

¹⁷⁶ Listing of the *Aarogya Setu* App on the Google Play Store https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_IN

Frontend Analysis through the Terms of Service & Privacy Policy



44. While registering, there is an “App Permissions” page, where at the outset there is an explicit acknowledgement of the sensitivity of the “topic. It states that the Government has taken steps to ensure a user’s “data is not compromised”. It avoids an explicit acknowledgement that such government practices are linked with people’s right to informational privacy. The permissions page makes three explicit disclosures:

- a. Device Location: The application, by default has access to the device’s location “always”. Users have the ability to change this setting.
- b. Bluetooth: Bluetooth is meant to be used to monitor device proximity with other devices using the Aarogya Setu app. Users are recommended to keep it on at all times.
- c. Data Sharing: Data generated through this application is shared with the Government of India only. It also clarifies that the user’s name and number will not be disclosed to the public at any time. However, this appears to be a much wider collection and possible sharing outside of the device, than envisioned under other apps.

Terms of Service (TOS) of Aarogya Setu

Broad permissions and data maximisation

45. As per the Terms of Service¹⁷⁷ the stated purpose of the application is to notify, trace and support app users if they have come in contact with other users of the application, who have tested positive for SARS-COV 2 (COVID-19). It is concerning that the purposes laid out here are vague enough to repurpose the app for multiple purposes. However, at the same time, it does make it worthwhile to question the Government's decision to monitor this data for compliance with quarantine or lockdown requirements.
46. Specifically, when two devices using the application are in range of one another, a protocol is initiated through which each device's personal information (including its location information) is stored on the corresponding device in a "secure" manner. How this data is secured is not apparent, but one would presume it is stored through an encryption protocol. One weakness is that unlike other protocols, which obfuscate these personal details of other users, there is no mention of the use of obfuscation technologies (like a temporary device ID) here.
47. Additionally, the Government appears to have real-time access to these interactions, which it is able to combine with people's individual health records that it has access to through the Indian Council for Medical Research (ICMR)¹⁷⁸. Through these two capabilities, if a user tests positive for the coronavirus, the Government may suo moto inform all users of Aarogya Setu who have come in contact with the concerned individual in the run up to the diagnosis. The period for the same is 30 days since diagnosis. A justification for this timeline of 30 days is not provided in the Terms of Service.
48. Users are required to allow the app to have access to the Bluetooth and GPS services of their device. The TOS also mentions, should users deny access to Bluetooth and/GPS it may lead to inaccurate or incomplete conclusions or decision making. People are also required to keep their device in their position at all times. They are also forbidden from sharing their devices with anyone else. The TOS says that if a user shares its device, it runs the risk of the user falsely being identified as COVID-19 positive.
49. We have multiple complaints with these conditions. First, the justification to collection and use of both GPS trails and Bluetooth proximity interactions is not provided-- and deviates from best practices which have been detailed

¹⁷⁷ Aarogya Setu, Terms of Use, <https://web.swaraksha.gov.in/ncv19/tnc/>

¹⁷⁸ As described on the ICMR website, it is the apex body in India for the formulation, coordination and promotion of biomedical research.

throughout this paper. However, the second issue evokes deep concerns. It is perhaps best to phrase it as a question. How will switching devices lead to a conclusion that someone is falsely identified as COVID-19 positive? Does this mean that people are categorised as COVID-19 positive based on the data collected by the application itself, instead of a formal test result to confirm a positive diagnosis? If this is indeed the case, there is a need to strongly commence dialogue to roll back the application and fine tune the entire process. These concerns are exacerbated by the fact that a recent report which interviewed people involved in the app's development disclosed that, without human supervision, algorithms determine the 'at-risk' assessment done by the app.¹⁷⁹

Severe restrictions undermine trust

50. The TOS of the application prevents the submission of misleading information about oneself. Given that there is a self identification test right at the beginning of registration, this would mean that the application collects a considerable amount of personal and sensitive personal data to use the app. Such a position is not aligned with the data minimisation principle.
51. The TOS prohibits users from tampering or reverse engineering the application. It also prohibits people from accessing information about registered users. Further, the TOS does not allow identifying or attempting to identify registered users or attempting to gain access to the application's cloud server. The relevant provisions in this regard, lack nuance. It prohibits good faith cybersecurity researchers and ethical hackers from stress testing the application and concomitant systems. It also prevents people from reverse engineering the application's backend source code, which prohibits the public from understanding what the application is trying to do.

Vague frameworks for discretionary action without objective standards

52. The disruption clause in the TOS allows the Government to temporarily or permanently suspend access to the application or its services. Further, the Government has the discretion to suspend it for all, or a certain class of users. Since this application is linked to people's health and right to life, such manifestly arbitrary powers to suspend or disconnect users is violative of people's fundamental rights under Article 21 of the Constitution. Moreover, a power to arbitrarily make decisions which affect people's fundamental rights, is inconsistent with the reasonable classification test under the Right to Equality protected under Article 14. Ideally, the provision should have clarified that should services (for all or a particular class of users) be suspended or down for a period of time, then the Government shall issue a notification which justifies the cause

¹⁷⁹ Karishma Mehrotra, *Behind Aarogya Setu app push: 'At least 50% people must download for impact'*, Indian Express, April 2020, <https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/>

of said suspension. The provision should offer clarity on the conditions under which a disruption is legitimate.

53. The TOS also has a blanket clause which limits the liability of the Government to any claims arising out of the use of the application. This includes no liability for Government should a person be unable to access or use the app; errors in contact tracing decisions vis-a-vis COVID-19 positive persons; and even for any unauthorised access/alteration to a user's information. This absolves the government from accountability. Specifically, it enables the unaccountable compromise to people's informational privacy and information security.
54. Finally, the TOS issued a disclaimer that the Government cannot be held legally responsible should the Aarogya Setu app and accompanying services lead to errors in accurately identifying people who have tested positive for COVID-19. Considering this disclaimer to hedge against the possibility of errors, it begs the question, who should users hold accountable should an inaccurate decision be made by the app which implicates a user's rights. This is a glaring oversight since earlier in the TOS we observe a provision wherein people can be falsely diagnosed as COVID-19 positive by the application of a personal device with someone, like a relative. This is another instance of the TOS being developed in a manner which enables lack of accountability and opacity.

Privacy Policy of Aarogya Setu

Ideal standards of a Privacy Policy

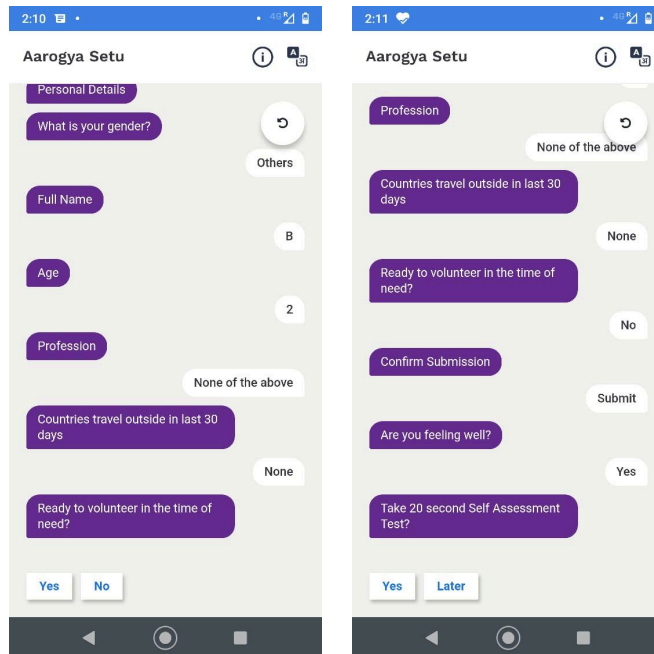
55. The contours of the privacy policy is to lay out contours of personal information collected, the manner in which it will be collected, and the purposes for collection. Ideally, Privacy Policies should nonetheless be consistent with known standards like Fair Information Practice Principles.¹⁸⁰ Briefly put, the privacy policy should adhere to:
 - a. Collection limitation principle;
 - b. Data quality principle i.e. the personal data used should be relevant to the purpose, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date;

¹⁸⁰ The Code of Fair Information Practices, Electronic Privacy Information Center (EPIC), https://epic.org/privacy/consumer/code_fair_info.html; Fair Information Practice Principles, International Association of Privacy Professionals (IAPP), <https://iapp.org/resources/article/fair-information-practices/>; The General Philosophy of the Fair Information Principles, Privacy First, <https://www.privacyfirst.nl/acties-3/item/154-the-fair-information-principles-canada.html>; Pam Dixon, A Brief Introduction to Fair Information Practices, World Privacy Forum, <https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>.

- c. Purpose specification principle, and this specification should be done no later than the moment of collection;
- d. Use limitation principle;
- e. Security safeguards principle;
- f. Openness principle;
- g. Individual participation principle;
- h. Accountability principle to give effect to the above principles

Information collected adopts an approach towards data maximisation

56. Coming to the Aarogya Setu App's Privacy Policy¹⁸¹, we notice certain key flaws. First, while registering, users must fill up a self-identification form. The form allows the application to collect several data points like (i) name; (ii) phone number; (iii) age; (iv) sex; (v) profession; (vi) countries visited in the last 30 days; and (vii) whether or not you are a smoker. These different data points connote personal and sensitive personal information about users. This information is transferred and stored in a cloud server. Notably, the level of personal information collected in this application is far beyond apps such as *TraceTogether* and the *Private Kit: Safe Paths*.



The image displays two screenshots of the Aarogya Setu app's registration interface. The left screenshot, titled 'Aarogya Setu', shows the 'Personal Details' section. It includes a 'What is your gender?' question with a dropdown menu and a 'None of the above' option. Below this are fields for 'Full Name', 'Age', 'Profession', 'Countries travel outside in last 30 days', and 'Ready to volunteer in the time of need?'. The right screenshot shows the 'Profession' section, which has a dropdown menu and a 'None of the above' option. It also includes a 'Ready to volunteer in the time of need?' question and a 'Submit' button. Both screenshots show a 'Yes' and 'No' button at the bottom.

Information exchange and storage opens up multiple threat vectors

57. When a user's device establishes contact (via Bluetooth and/or GPS) with another device, the two devices exchange information with each other to

¹⁸¹ Aarogya Setu, Privacy Policy, <https://web.swaraksha.gov.in/ncv19/privacy/>

confirm an interaction. The exchanged information is a combination of the personal information of the other registered user, the location coordinates and a timestamp of the interaction. The Privacy Policy also reveals that the application collects the phone's location data and maintains a record of all the places the user may have visited. Along this trajectory it also maintains records of contact the user may have made with other users of Aarogya Setu. This exchange of information of personally identifiable information among people's devices certainly adds to the vulnerability. It adds to the number points of attack for malicious actors. Also, there are no mentions of efforts to obfuscate this information in the form of a temporary device ID.

Purpose limitation is undercut by its exceptions

58. The Privacy Policy's disclosure with respect to the use of collected information warrants scrutiny. In one voice it states that people's personal information¹⁸² collected by the application will be stored locally on the device. However, it lays down certain conditions in which said information may be uploaded to an external server (in the cloud) and used by the Indian Government.
59. At a first level, it does not specify which department or ministry or officials will be the ones accessing that data. Such lack of specificity adds to concerns of overreach. Coming back to the conditions under which personal information can be transferred to a cloud server for the use of Government:
 - a. First, this may be done to create "aggregated" datasets of "anonymised" data, to generate reports/heat maps and other similar statistical visualisations for COVID-19 management. Unfortunately, there is no supporting texture on what the Government views as "anonymised". Considering the application collects several different data points, there is an onus to address the technical risk of re-identifiability. It will allow technologists to guide them on how to approve its systems. Further, the Government should disclose the computational technique it is deploying to obfuscate the data. Secondly any aggregated datasets, should be accompanied with texture on how it is built and what safeguards are being taken to ensure that there are no risks of discrimination against minorities and at-risk communities.
 - b. Additionally, the Privacy Policy contains an enabling provision which allows the Government to export people's raw personal information in case a user has either tested positive for COVID-19 or had "close contact" with a person which has "tested positive" for COVID-19. It is important that the application confirms via its TOS as to what it means by "testing positive", considering there is a reference made to false positives if devices are switched between people. Such clarity will help external

¹⁸² (i) name; (ii) phone number; (iii) age; (iv) sex; (v) profession; (vi) countries visited in the last 30 days; and (vii) whether or not you are a smoker

parties in understanding the data collection capabilities the state is granting itself.

- c. The Privacy Policy also fails to adequately restrict its scope of purpose limitation. The primary purpose is to inform users if they are at risk of COVID-19 exposure. However, the Government is also allowed to share the personal information with “other necessary and relevant persons”, for “necessary medical and administrative interventions” which suggests interdepartmental exchanges of people’s personal information. This is more excessive than countries like Singapore and even Israel. It is essential the Government provide supporting texture to such clauses, else it enables vagueness which can allow for opaque functioning of the state with no accountability. As discussed earlier in this paper, opacity is what fuels the creation of surveillance systems.
- d. Further, people’s personal information may be used for compliance of legal requirements. This suggests it may be usable for enforcement purposes as well, a measure which contradicts the position of many democratic countries which are considering or already deploying contact tracing solutions.

Data Retention for now and forever?

60. The Privacy Policy indicates that the Aarogya Setu application will delete all time stamped records of user contact after 30 days on a rolling basis with certain caveats. However, it also states that the data deletion requirement does not apply in any capacity to anonymised and aggregated datasets. This is a first step towards permanent government architectures.
61. When it comes to personal information, the Privacy Policy indicates that people’s personal information even after uninstallation of the application for a period of time, for purposes, “... for which the information may lawfully be used or is otherwise required under any other law for the time being in force.” This clearly does not suggest intent on the part of the Government to destroy these systems. As a result there is a risk the personal information of users may be held for the duration of this public health crisis and beyond.
62. More importantly, the Privacy Policy fails in providing users the right to formally request for their data to be deleted. It even fails to provide users with an opportunity to audit if representations that their data has been deleted.

User Rights exist to seek deletion. That’s it.

63. Positively, the Privacy Policy states that should a user cancel their registration, then in the ordinary course of circumstances, all personal information will be deleted after 30 days from the date of termination. There is a need to integrate a mechanism for users to audit this and check the status of their records being

deleted/stored. Further there are no provisions to deal with users having a clear right to seek copies, correction and modification of their personal data.

Data Security Safeguards exist but remain unverifiable.

64. The Privacy Policy indicates that in order to securely collect, store, transfer and process personal information and related records, the Government is deploying encryption to secure data in both transit and rest. There is a need for greater transparency and clarity on this, with regard to encryption and obfuscation techniques which may have been deployed.
65. From an information security standpoint it is important for the Government to also build systems to prevent manipulation of the application. There exist theoretical risks of malicious actors gaining remote access and falsely notifying app users of contact with COVID-19 positive persons. Therefore, stakeholders should be apprised of the systems being deployed to ward off information security and information warfare risks as well.

Establishes a system for remedy by provisioning for a Grievance Officer

66. On a positive note, the Privacy Policy prescribes a designated grievance officer for user complaints. This duty is being performed by a Deputy Director General at the National Informatics Centre (NIC). To improve this functionality, users should be able to write to this officer to audit the use of its personal data, and exercise control over it, consistent with the individual participation principle¹⁸³ of the FIPPs. Furthermore, there should be a clear transparent basis for how such complaints will be handled and to what volume institutional capacity exists to deal with the volume of complaints which are likely to arise given the intended number of installs Aarogya Setu is intended to achieve.

Vagueness on data transfers

67. The Privacy Policy ostensibly states that people's personal information cannot be transferred to third parties. But this is subject to conditions of transfer which have already been stated in the Privacy Policy. This would mean third parties may have access to anonymised datasets.
68. Further, third parties may even receive access to people's personal data should they test positive for the coronavirus or have made contact with another user

¹⁸³ An individual should have the right:

- a) to obtain confirmation of whether or not the data controller has data relating to them;
- b) to have data relating to them communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to them;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and
- d) to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended;

who has tested positive for COVID-19. In this context, third parties may receive access to personal information, to support “... *necessary medical and/or administrative purposes*”. Ideally, third party access to people’s personal information should not be allowed.

69. However, if it is then the Government must create necessary mechanisms which ensure third party access to these datasets are restricted strictly by purpose and time. For the sake of transparency the government should clarify what constitutes necessary medical and administrative purposes in the context of COVID-19.

Urgent need for transparency and clear limits

70. When it comes to the actual processing of personal data the European Data Protection Board clarifies that personal data which needs to be processed to respond to the crisis, may only be processed for specified and explicit purposes. Moreover, there should be clear information provided to individuals with respect to the purposes of processing and the retention period for collected data. In addition there is a need to detail security measures and confidentiality policies towards ensuring there are no unauthorised disclosures of personal data.
71. As such the *Aarogya Setu* application appears to clearly be inconsistent with privacy-first efforts which are being considered by technologists and governments as discussed in earlier this paper. There is a need for Indian stakeholders to study these different initiatives and pick an evidence-based path which nevertheless protects people’s right to informational privacy. For instance, there is a need to justify how the use of both Bluetooth and GPS is necessary without overtly compromising on people’s privacy. Moreover, the government with the inputs of healthcare experts and epidemiologists must justify the efficacy of systems like *Aarogya Setu*.
72. Unfortunately, it may be argued that despite its best efforts, the Government of India’s current initiative appears to be a combination of countries like Singapore, Taiwan and China. It certainly contrasts with how most countries are taking their time (over several weeks or even months) in ensuring that they deploy “privacy-first” contact tracing technologies. Conversely, the Indian application was ready for download by Indians within two weeks from the day the first line of code was written (March 19 - April 02), 2020.¹⁸⁴
73. More fundamental issues subsist when it comes to transparency with respect to the app. First, there is no effort to either disclose technical details regarding the

¹⁸⁴ Karishma Mehrotra, *Behind Aarogya Setu app push: ‘At least 50% people must download for impact’*, Indian Express, April 2020, <https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/>

app or the underlying source code for public scrutiny. Similarly, the app's TOS explicitly prohibits any kind of re-engineering of the platform. Should a researcher undertake such activities in good faith, rather than focus on scope for improvements, the state may take some action against such parties. Finally, we face issues with a possible black box in algorithmic decision making which implicate people's rights and fundamental freedoms i.e. freedom of movement.

74. Thus, there is a need to immediately rollback the application or expedite measures to improve the app's design and deployment in terms of trust, security and informational privacy. In addition, in the pursuit of transparency and auditability, the Indian Government should follow Singapore's lead and release the source code of the *Aarogya Setu* application. This would allow technologists to scrutinise the government's practices and provide technical suggestions on how their efforts may be improved or alternatively rolled back.

Imperatives for Rule of Law Compliant Contact Tracing

75. Based on the analysis presented so far, it is reasonable to conclude that the Government of India has a duty to ensure that its contact tracing efforts are consistent with the rule of law. For instance, a lot of initiatives (including public-private endeavours) not just in India but across the world are taking place in an extra-legal manner. India of course suffers from a distinct disadvantage. It does not have a comprehensive personal data protection framework, nor a rights compliant surveillance interception framework.
76. However, even in times of emergency we must benchmark government interventions which restricts people's privacy against the rule of law. This law stems from the Hon'ble Supreme Court of India's landmark judgement in *KS Puttaswamy (Retd) and Anr v Union of India* [(2017) 10 SCC 1]. Specifically, it clearly states that even when responding to an epidemic or public health crisis, there is an onus on the state to use people's health information in a manner which preserves their "anonymity". This means going beyond a basic level of obfuscation, but adopting technical best practices towards anonymisation which make re-identification difficult even for malicious actors. Any representation that privacy requirements do not apply to anonymised datasets must therefore be viewed through a sceptical lens.
77. However, even should the state be able to successfully do this, any actual restriction to people's privacy must be compliant with thresholds for reasonable restrictions to the right to privacy. The means that government contact tracing activities must take place under a clear legal regime, for a necessary purpose, in a manner where the restriction is proportionate (least restrictive alternative), along with procedural safeguards to ensure accountability and prevent abuse.
78. To demonstrate compliance with these requirements, limits and transparency are a prerequisite. Moreover, it must be consistent with the requirements of public health responses. In this regard, some guidance may be taken from recent

recommendations of the European Commission on a common tool box for the region to use technology and data in response to COVID-19. In particular the recommendation includes the deployment of mobile applications and the use of anonymised data to map mobility.¹⁸⁵

79. The European recommendations say that even in a crisis of this magnitude, technology based interventions must respect people's fundamental rights and freedoms, including the right privacy, guaranteed by the EU legal order. In this regard, any restrictions by European governments must be justified and proportionate. This means they must necessarily be temporary and strictly limited to what is required to combat the crisis, and cannot exist after this crisis has passed.
80. This includes a strict adherence to data minimisation. Particularly it discusses the use of this data by public health authorities and research organisations, rather than a gamut of private sector and government departments. The European Commission also aims to ensure that the region ensures technology deployments for the novel virus remain decentralised in terms of design and seek to empower citizens. Governments should facilitate methodology monitoring, and similar access to the public on details regarding the effectiveness of these applications.
81. Most notably, the European Commission says that data collected through these applications cannot allow surveillance and stigmatisation. Specifically, there should be strict limits in terms of purpose limitation and the data collected through these systems cannot be used for law enforcement or commercial purposes. There should be regular review, in which objective assessments are made evaluating the need to continue maintaining such systems even during the duration of this crisis.
82. In India, predefined sunset clauses, along with Parliamentary oversight would be helpful toward this. The systems should be designed in a manner where once the purpose is no longer applicable, the systems stop processing personal data, and the Government can irreversibly destroy such systems and the personal data which has been collected and/or used. The European Commission explicitly notes that in order to satisfy purpose limitation requirements, it will propose to countries to not process location data or map people's movements. It will urge European states to use proximity data i.e. technologies like Bluetooth.

¹⁸⁵ European Commission, *Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, C(2020) 2296 final, April 2020,

https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

Recommendations

83. Additionally, stakeholders must also appreciate that government deployment of novel technologies to automate contact tracing upends how contact tracing works in the physical world. In an outbreak of disease of any scale, contact tracing is premised on tracking and containing the spread of the pathogen. Strategies are curated based on the manner of transmission of the pathogen itself.
84. Once a particular person is infected (confirmed by a test), authorities isolate this individual. The next step is identifying contacts in the period of incubation and testing them. Those who test positive are isolated and the process is repeated.¹⁸⁶
85. The purpose for contact tracing is containing the spread through specific knowledge of fact which is confirmed with a positive test. When it comes to contact tracing applications like *Aarogya Setu*, people may be notified that they are at risk of exposure to a particular pathogen, in this case the coronavirus, at times without the definitive confirmation which comes with a test.
86. The Government must be alert to the possibility that people who are notified of a possible risk exposure via the *Aarogya Setu* app may not have any ready available avenue for treatment. How people react to a circumstance like this is unpredictable. India has already seen one outcome wherein the government failed to preempt the migrant labour exodus at the start of its national lockdown. It is suggested that it does not repeat such mistakes, and factor in unintended consequences of the app's design features.
87. For example, an unintended consequence with the design of the application as it stands, could be that people panic and flood healthcare centres which may stress scarce testing and treatment resources. If the application's design does not factor in such eventualities there is a risk that the application may inadvertently hurt capacities to treat actual confirmed cases.
88. In this regard, it may be noted that even in biomedicine disease surveillance must adhere to ethics standards. It is suggested that India's technological surveillance for disease containment also adheres to best practice standards and protect people's privacy. Towards it is proposed that the Government of India:
 - a. Establish the primacy of the Ministry of Health and Family Welfare (MoHFW) as the convening agency for technology deployment to contain the spread of COVID-19. They should collaborate with state level health departments, and the Ministry of Electronics and Information Technology (MeitY) since they are the nodal authority for technology related aspects

¹⁸⁶ Sean McDonald, *The Digital Response to the Outbreak of COVID-19*, Centre for International Governance Innovation, March 2020, <https://www.cigionline.org/articles/digital-response-outbreak-covid-19>.

to this conversation. Further, all committees which are set up to work on this project must be transparently disclosed along with a detailed publication of its Terms of Reference.

- b. Assure citizens, that inferences which are gleaned from this application will not be used for law enforcement or criminal investigations.
- c. Ensure that applications like Aarogya Setu are administered a special legislation which is enacted for this purpose, consistent with the requirements of the right to privacy test outlined by the Supreme Court of India in its judgement in *KS Puttaswamy v Union of India* which has been detailed in this report.
- d. Ensure that the systems adhere to principles of data minimisation and purpose limitation by ensuring that the information collected from the *Aarogya Setu* will not be collated with other information repositories, since integration of databases makes deleting more difficult later. Assure people that these are not permanent systems, and set up a sunset clause feature (with a defined timeline) in the special contact tracing legislation, to ensure that these systems will be deleted.
- e. Build in Fair Information Practice Principles into the Terms of Service and Privacy Policy. Further, implement changes as suggested in prior sections of this working paper to ensure that citizens can hold the Government accountable in its use of these contact tracing systems. People should be granted an avenue to seek timely judicial remedy if the need arises.
- f. Ensure that people have control over their personal information, and have the agency to get tested, and confirm if they are indeed infected by the coronavirus. Predictive models as deployed in China are dangerous to people's civil liberties and fundamental freedom and have to be avoided. Citizens should have the agency to share information via contact tracing applications to inform its citizens. This should not be a coercive exercise. If indeed such systems are effective, then it is the responsibility of the Government to instead invest in information dissemination campaigns to encourage socially responsible behaviour and share their information with the application.
- g. Ensure that the data should primarily reside on people's devices, where effective obfuscation techniques are deployed. The application should not be able to map people's movement and/or location, but rather focus on establishing proximity. The application should be about empowering users, whether they are safe or not. If data is exported to an external server, this should be at the behest of the user, where the consent should be meaningful and informed.

- h. Publish the protocols based on which algorithmic decision making takes place. This should indicate if there is human supervision, and other safeguards which are being deployed.
- i. Publish the application's source code, and specifications with respect to Bluetooth, cryptography, anonymisation, aggregation of anonymised datasets and so on. It should also encourage security researchers to undertake good faith penetration tests, to support the Government in preventing attacks against malicious actors.
- j. Allow people to check, correct and delete, their personal information which has been used by the application. Second, they should have a defined through which can audit if the Government has in fact adhered to personal data deletion requests.
- k. Ensure that the TOS and Privacy Policy of the *Aarogya Setu* application remove the exceptions to Government processing of personal and anonymised information for indefinite periods and vague purposes. Similarly, remove exemptions for non-deletion of records after the 30 day time period has elapsed.
- l. Halt the collection and processing both GPS trails and Bluetooth trails since this is not the least intrusive means to establish contact between two individuals.
- m. Publish an accompanying website and manifesto which contains all the processes, deployments, plans and justifications for the *Aarogya Setu* application.
- n. Justify the use of surveillance technologies and establish nexus between such deployment with the public health response that the Government is undertaking. Since this is an intrusion into people's civil liberties this nexus must be established with the support of empirical data, and also articulate the degree to which these technological deployments will support India's relief efforts. There should be periodic review assessments.
- o. Reduce the number of personally identifiable data points collected of each application user to the strict minimum necessary.
- p. Publish detailed plans of the Government of India on how it intends to ensure that this will not be a permanent system for creation of "rich" datasets. Rather, it should articulate plans on how the Government of India will ensure that any data collected in an external server is designed to be deleted and that it won't be integrated with other databases.
- q. Additionally, clarify which agencies of Government of India have access to these databases, and provide justifications as to how each department's

access to these databases is aligned with the thresholds of necessity and proportionality.

8. A partnership of (silicon valley) giants

Background of the Apple and Google partnership

1. Stakeholders have been suggesting that instead of risking the creation of new surveillance systems, there is value in considering infrastructures/pathways which already exist. In this context, they suggest that there are certain parties which have unfettered access to people's proximity (and location data). In particular, they refer to telecom providers and of course major mobile phone operating system (OS) providers like Google and Apple.¹⁸⁷
2. These stakeholders suggest that OS providers could facilitate privacy-preserving and interoperable contact tracing/location tracking features. They also suggest that such providers are better equipped and have greater experience in reliable obfuscation technologies like differential privacy¹⁸⁸ or homomorphic encryption. Such suggestions are made with the accompanying request that any such contact tracing deployment is accompanied with a suitable regulatory framework to keep the OS providers accountable.¹⁸⁹
3. Such demands are also reflected in an open letter from American medical professionals, epidemiologists and technologists. Among other things, they have requested OS vendors provide an opt-in, privacy preserving OS feature to support contact tracing to enable self-quarantine, monitoring, early detection and prevention of tertiary cases.¹⁹⁰

The announcement

4. On April 10, 2020, Apple and Google announced a partnership where the two firms will collaborate on an interoperable contact tracing partnership.¹⁹¹ The two

¹⁸⁷ Jon Evans, *Test and Trace with Apple and Google*, Tech Crunch, March 2020, <https://techcrunch.com/2020/03/29/test-and-trace-with-apple-and-google/>

¹⁸⁸ Jun Tang and others, *Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12*, 2017, <https://arxiv.org/abs/1709.02753>.

¹⁸⁹ Jon Evans, *Test and Trace with Apple and Google*, Tech Crunch, March 2020, <https://techcrunch.com/2020/03/29/test-and-trace-with-apple-and-google/>.

¹⁹⁰ 13 things tech companies can do to fight coronavirus: An open letter from technologists, epidemiologists & medical professionals, March 2020, <https://stop-covid.tech/>.

¹⁹¹ Read Generally, Mark Gurman, *Apple, Google to Bring COVID-19 Contact Tracing to 3 Billion People*, Bloomberg, April 2020, <https://www.bloomberg.com/news/articles/2020-04-10/apple-google-bring-covid-19-contact-tracing-to-3-billion-people>; *Apple and Google Partner on Covid-19 contact tracing technology*, April 2020,

OS providers have the scale to potentially provide these facilities to around 3 billion smartphone users globally. This contact tracing system is being positioned as a voluntary “opt in” system.

5. This solution will be designed to notify users if they have come in contact with an infected individual, along with a recommended course of action which may range from quarantine to self isolation. Demonstrating the long term nature of the global response to COVID-19, the plan is to introduce the system in two phases.
 - a. In **Phase 1** (to commence in May, 2020) public health authorities will be given the capability to run apps in which iPhones and Android phones will be able exchange information anonymously with one another. The design will allow users of the public health app to voluntarily notify the system if they test positive for COVID-19. Then users which were in close proximity in the last few days will be notified that such contact was made. The default timeline for this check will be 14 days. However, health authorities will have the discretion to amend this.
 - b. **Phase 2** will be administered over the course of a few months. This update to the programme will essentially reflect the recommendations discussed earlier. The contact tracing software will be embedded into the operating system itself, which removes the need for users to download an application. This functionality will also be opt-in but the potential for this solution to scale is enormous and brings with its own set of opportunities and risks.

Technical features of the partnership project

6. To reassure people on privacy, Google and Apple stressed on the fact that consent will be baked into its design and they will not collect location data.¹⁹² The statement also stresses that users will not be informed whom they came in contact with, or where the contact takes place. The companies will also not be able to access this data and the entire system can be shut down, if required. American lawmakers have expressed concern with the project since this may

<https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>.

¹⁹² Read Generally, Mark Gurman, *Apple, Google to Bring COVID-19 Contact Tracing to 3 Billion People*, Bloomberg, April 2020, <https://www.bloomberg.com/news/articles/2020-04-10/apple-google-bring-covid-19-contact-tracing-to-3-billion-people>; Apple and Google Partner on Covid-19 contact tracing technology, April 2020, <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>

involve federal, state and local authorities collaborating with large tech platforms which store in its servers large reams of sensitive personal information.¹⁹³

7. Similar to Singapore's *TraceTogether* application and other projects discussed in this paper, the proposed project will be based on Bluetooth. Once contact is established, devices exchange anonymous device identifiers (which are updated for every user's device on a daily basis), which confirm a timestamped interaction. To enhance people's privacy, anonymous digital identifiers change roughly every fifteen minutes.
8. Should an individual test positive for COVID-19, the person has the ability to enter their diagnosis into a corresponding app which is designed for health agencies. This application then must seek the consent of users to export their "close proximity" interactions which have been recorded in the days prior to diagnosis. This data which has been exported is stored temporarily in a remote server for 14 days.
9. When it comes to the devices of the people who have made contact with this diagnosed person, the process flow is as follows. First the phone will check the server periodically to assess if any of its identifier keys are linked with COVID-19 positive cases. All positive keys are downloaded back on to this individual's phone and matched anonymously for validation purposes. When matched, a notification is sent to the other person's phone along with suggestions from health agencies on how they can quarantine and self-isolate.

Sequencing of the project

10. To effectuate this project the solution will release a series of Application Programming Interfaces (APIs) and OS-level technology to enable the contact tracing, as described above. The initial apps (built on the APIs) will be available for download via respective app stores. Eventually, they intend to move away from APIs and broaden this platform by integrating it into the underlying operating system.
11. The project aims to create a common standard of interaction between different technologists and public health authorities across the world. The two firms state that privacy, transparency and consent will be underlying pillars of this project. The actual solution will also be informed by the inputs of other stakeholders. To further transparency, they have published specifications for Bluetooth,

¹⁹³ Mark Gurman, *Apple, Google to Bring COVID-19 Contact Tracing to 3 Billion People*, Bloomberg, April 2020, <https://www.bloomberg.com/news/articles/2020-04-10/apple-google-bring-covid-19-contact-tracing-to-3-billion-people>

cryptography (i.e. encryption) and API frameworks.¹⁹⁴ As of now information on accountability mechanisms remains difficult to discern.

Unique risks due to private sector initiative

12. Just a day before this announcement Professor Ryan Calo made a prophetic deposition before US lawmakers on the risks of involving big tech in the fight against the coronavirus.¹⁹⁵ He dedicates considerable space to the deployment of contact tracing applications by big tech companies.
13. In this context, he highlights that at a fundamental level, a contact tracing technology solution necessitates the processing of highly sensitive personal information i.e. health data, and either insights on movements and/or interpersonal communications. Unlike the prior projects studied in this paper, which were either steered by Government and not for profit researchers, there is the added complexity here when private sector behemoths are involved.

Enhanced need for checks and balances

14. Any private sector driven response to digital contact tracing must adequately tackle issues of transparency, consent, purpose limitation, and corporate objectives. There is an enhanced need for scrutiny of security practices if there are any plans to share sensitive personal information like health data with other private actors. Calo effectively questions the efficacy of such projects on two discrete grounds:
 - a. First, in case there are a low number of installations and a particular contact tracing application is not widely used, then there is a risk of false sense of security among users, who may be more cavalier with respect to their movements.
 - b. Second, it cannot possibly give a clear picture of the contagion risks since these solutions do not account for the considerable role played by asymptomatic carriers in the spread of the disease.
15. Whereas, even when private actors are entrusted for such projects, there is a need to engender public trust. Name recognition and brand of course, help with this trust, but trust also covers facets like safety, privacy and reliability. At a minimum these businesses must also have to comply on principles of (1) specific limited purpose, where there is a specified end data and a defined outcome to

¹⁹⁴ Apple and Google, Privacy Preserving Contact Tracing, April 2020, <https://www.apple.com/covid19/contacttracing/>.

¹⁹⁵ Ryan Calo, "Enlisting Big Data in the Fight Against Coronavirus", Senate Committee on Commerce, Science, and Transportation, April 2020, <https://www.commerce.senate.gov/services/files/D069F0C0-2B67-4999-AC75-5BC41D14D00C>.

the project; (2) complete transparency; and (3) strong enforcement mechanisms which can hold these businesses accountable and protect people's fundamental rights to informational privacy.

16. Stringent checks and balances are important to consider, since the creation of new systems, even if they are characterised as temporary, are difficult to roll back. Aside from these general risks, when analysing the project announced by Apple and Google, we must stay vigilant in a few distinct ways.

Negotiating government use of personal data

17. The project discusses a system wherein once users of the application are diagnosed with the novel coronavirus, they can export their records from the prior few days on to an external server. This external server allows public health officials to access relevant records. Since, this means health departments in governments are granted access to people's personal data, there is an onus to ensure use limitations.
18. Under the guise of contact tracing, health authorities should not be allowed to share such information and insights towards civil liberty restrictions. For example, Apple and Google will have to update the public on how its systems can and cannot be used by governments. For instance, how does it resolve civil liberties risks associated with government use of these sensitive personal interactions to enforce lockdowns and quarantines? Similarly, health authorities should not be able to share these insights with other government departments and repurpose it for other objectives like law enforcement or criminal investigations.
19. On April 13, 2020, reports confirmed that Google and Apple are working with the technology arm of the UK's National Health Service (called NHSX) in developing a contact tracing application.¹⁹⁶ Responding to the story, the UK Government has confirmed that a contact tracing app will be pilot tested in one week.¹⁹⁷ Therefore, there is a need to have an expedited conversation on how such partnerships between private actors and public authorities implicate people's rights, and how the public may hold them accountable.

Issues of Competition and conflicts of interest

¹⁹⁶ Tim Shipman and Nick Rufford, *NHS phone app holds key to lifting UK's coronavirus lockdown*, The Times, April 2020, https://www.thetimes.co.uk/edition/news/nhs-phone-app-holds-key-to-lifting-uks-coronavirus-lockdown-wfnt3pt0g?wgu=270525_54264_15867423998798_15becce016&wgexpiry=1594518399&utm_source=planit&utm_medium=affiliate&utm_content=22278

¹⁹⁷ Leo Kelion, *Coronavirus: UK confirms plan for its own contact tracing app*, BBC, April 2020, <https://www.bbc.com/news/technology-52263244>

20. Competition authorities and policymakers must carefully scrutinise this project, in an ex-ante manner. This is because it may severely deter competition and innovation in a crucial area of urgent public interest. There is a need to consider conflicts of interest at two levels. In the project's first phase, Apple and Google will be competing with other applications developed by other groups, companies, consortiums, researchers, and governments. In this context, there is a need for oversight on how *App Store* and *Play Store* treats its application in comparison to other similar solutions.
21. Second, as the project evolves and integrates itself into the operating system, we need to evaluate what it will mean for innovation in the space. Does the project envision a means to be interoperable with other operating system providers in smartphone and feature phone markets.
22. The utility of such solutions are defined by network effects, large scale adoption and overall stickiness. Therefore, will the entry of Apple and Google in a partnership capacity squash out any current and future competition? Further, stakeholders must ask themselves will it deter other stakeholders from developing better privacy respecting solutions?
23. Whatever the answer, it should not leave us in a paradigm with one digital contact tracing solution where large technology firms and governments have unimpeachable control over the system. To mitigate such risks, there may be an overriding need to administer ex-ante impact assessments-- both economic and rights oriented to consider the implications of the project before it is deployed. Based on the findings, there may be a need to intervene and control such firm behaviour.

Should such projects be controlled by trans-national corporate entities?

24. If it is allowed to proceed, the project should be defined by end dates. It should be conceptualised in a manner where any centralised system is geared towards deletion. There should be no risk that these systems become future systems of perpetual surveillance. This includes perpetual surveillance by private actors.
25. Here, it is beneficial to frame the issue of private sector surveillance through the lens of *surveillance capitalism*. Shoshana Zuboff in her tour de force account in *The Age of Surveillance Capitalism*,¹⁹⁸ describes challenges with incursions by big tech into people's personal lives. She describes the notion in stages. Through these subtle incursions into the personal space, private personal information is collected.

¹⁹⁸ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the new Frontier of Power*, Public Affairs, 1st Edition, 2019

26. Once it is sufficiently amassed there is a sufficient reservoir of information beyond what is needed for systems improvement which has been termed as a “behavioural surplus”. Zuboff with immense empirical backing describes “behavioural surplus” as follows. Some of the behavioural data which is collected by these firms toward service improvement. But this constitutes, but a tiny fraction of the behavioural data which is collected.
27. The remaining reservoir of insights serves nothing more than as a surplus, which is worked on by machine intelligent systems which facilitate the creation of prediction products. These products are traded in what Zuboff coins as “behavioural futures” markets, where parties place bets, and ultimately seek to shape future human behaviour. An intuitive way to think about this is targeted advertising or information dissemination.
28. Considering the nature of sensitive personal information which would be involved in this proposed project we must consider how to limit opportunities for perpetual profiteering. Stakeholders must deliberate on fetters on the use of any personal data exported into external servers. Similarly, there must be limits towards the ultimate destruction of these datasets.
29. At a more fundamental level, it is also important to consider the validity of such projects being administered in a purely corporate structure. Considering the pre-existing scale that Apple and Google enjoy in the smartphone market, without interventions, it would in all likelihood become the default user choice for contact tracing. There is an inevitability to that outcome.
30. Considering the overarching public interest in global responses to COVID-19 and the human rights implications of contact tracing, should these solutions and the supporting infrastructures, be categorised as public digital infrastructures? Instead, should there be regulated access to public-private models? Or should it merely be regulated opportunities for private actors to participate? While the model remains unknown, there is a need to have an expedited conversation on this front.
31. The conversation must revolve around two fronts. First, is there a need to install broad based and inclusive institutional structures to audit the activities and hold such corporate endeavours accountable. Secondly, we need an open dialogue on whether firms like Apple and Google with extraordinary technological capabilities and resources can support global responses to the pandemic in a philanthropic capacity, which is divorced from their overarching corporate interests.

Conclusion and final recommendations

1. As discussed in this paper, the role of technologies in steering responses to the coronavirus present complex challenges to democratic rights. India lacks a comprehensive data protection law and has not reformed its surveillance frameworks¹⁹⁹ in line with the right to privacy. In addition to the specific recommendations and analysis present in the working paper, it may be prudent to juxtapose technology's regulatory limitations with an allied domain in this crisis, namely bio-medicine.
2. While the world is becoming intimately familiar with the steps, process and rough timeline towards the discovery of a vaccine to SARS-COV2, the same cannot be said with respect to technology deployments. A clear reason for this contrast is that the regulatory framework for companies to manufacture drugs and medication are clearly defined. Therefore, even under expedited timelines there is an entire process to ensure quality assurance, trust, safety and ethical oversight of the ultimate medication. The same goes for disparate segments like automobile manufacturing, cosmetics development or even social science disciplines like psychology.
3. By comparison, the regulatory immaturity of technology markets mean that similar safeguards do not subsist. It is compounded by the fact that solutioning in the domain, tends to regularly clash with civil liberties and democratic guarantees. An effective rule of thumb in discerning good practices from bad ones was recently articulated by Sean McDonald. In an article on the issue with technology responses to COVID-19, he states that good practices are rigorous, contextually tested, and work within the structures of existing expertise and accepted best practice approaches. Conversely, a bad practice is one which will try to adopt approaches which circumvent, or even question the integrity of these best practices.²⁰⁰
4. In technology markets public institutional review is necessary toward quality assurance and the preservation of basic rights.²⁰¹ However, a criticism which may arise in the context is that solutionism and the present pace of development is needed to stem the pace of this unprecedented pandemic. Such an objection

¹⁹⁹ Which currently operate under outdated laws like the Telegraph Act, 1885 and the Information Technology Act, 2000

²⁰⁰ Sean McDonald, *The Digital Response to the Outbreak of COVID-19*, Centre for International Governance Innovation, March 2020, <https://www.cigionline.org/articles/digital-response-outbreak-covid-19>.

²⁰¹ Sean McDonald, *The Digital Response to the Outbreak of COVID-19*, Centre for International Governance Innovation, March 2020, <https://www.cigionline.org/articles/digital-response-outbreak-covid-19>.

arises from an assignment of value in which the danger posed by mass surveillance to democratic freedoms is assigned a lower score against the ostensible utility of technology interventions. This leads to outcomes in favour of public policy choices made without objective, evidence based evaluation. A perverse outcome tends to the deployment of technological and data analysis systems, without any semblance of a review as to its efficacy.

5. Here rests certain risks which must be considered seriously for the health of the wide spectrum of fundamental rights, each one of which link to the fundamental right to privacy as articulated by the Hon'ble Supreme Court of India. These risks become exaggerated in contexts where experimental data amassing projects are being deployed into vulnerable contexts, without checks and balances. Technology deployments tend to be more effective when the target is limited to adding capacity or efficiency to an existing practice/technique. But what about scenarios where technology seeks to reinvent the wheel? Or develop proxies for known systems of trust, in pursuit of speed and efficiency?
6. India faces a grave challenge today not only to the health of its people but also to the nature of its polity. It has to ensure that emergency situations like a rapidly evolving public health crisis does not institutionalise centralised, long-term, unchecked and open-ended power structures. Many of these frameworks when placed within technical systems will wield power in ways that will undermine constitutional checks and balances. These are not hypotheticals. As per a recent report the central government is contemplating using the application as an e-pass to travel within the country.²⁰² Combine this with the fact that its risk assessments are done through unsupervised algorithms and we are looking at a template which mirrors China's AliPay Health Code.
7. In this context, it is useful to refer to an essay by Professor Hu Yong²⁰³ which critiques the Chinese deployment of surveillance in responding to the coronavirus. Professor Yong is from Peking University's School of Journalism and Communication. In his prescient essay entitled, "*The Public Interest and Personal Privacy in a Time of Crisis*", he evaluates pathways for the Chinese government to reconcile the public interest with personal privacy.²⁰⁴ His observations are important for stakeholders to consider in Asian democracies.

²⁰² Aparna Banerjee, *Aarogya Setu app can be used as e-pass to facilitate travel amid lockdown: Modi*, Live Mint, April 2020, <https://www.livemint.com/technology/tech-news/aarogya-setu-app-can-be-used-as-e-pass-to-facilitate-travel-amid-lockdown-modi-11586605016598.html>

²⁰³ A combined interpretation of the ChinAI newsletter and a Google translation from Chinese (simplified) to English of the original article. Any errors in interpretation are the author's alone.

²⁰⁴ Hu Yong, *The Public Interest and Personal Privacy in a Time of Crisis*, March 2020, <https://mp.weixin.qq.com/s/2KRGP2ErKlQ9XF98asy8-w?fbclid=IwAR24LIWvXNkxjR69sKsduoPp9cVwSCsMthAYCXXdUoqC3mooPvLWZYGIk4> & https://docs.google.com/document/d/1Lvuox6N_g_j6lL-ohD0WStaYmZl7x6wyxibqd7cA9cU/e_dit?pli=1

8. History is littered with many examples across the world where surveillance tools fail to exercise caution, and stay within limits, owing to the benevolence of the state. The US has its history with the creation of data amassing infrastructures in a post 9/11 world, and after the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, which is commonly abbreviated to as the USA PATRIOT Act. Similarly, India has its own experience with Aadhaar, whose issues with purpose and scope limitation is expansively documented.
9. Therefore, in the public interest, while there can be no denying that technology may have a role to play in the global response against this pandemic, there is also a complementary public interest in protecting individual freedoms for the long term. Why? The answer is simple, individual freedoms like the right to privacy are key constituents of democratic societies. Therefore, even as the state makes some intrusions into people's personal spaces, during this time of crisis, it has a competing obligation to assure all stakeholders that these incursions are justified and will not be permanent.
10. How can this manifest tangibly? States must function within a rule of law framework. Further, Yong astutely mentions that there is a high degree of responsibility of the state to ensure intrusions to the right to privacy are consistent with Fair Information Practice Principles which were ultimately crystallised in the 1980 Privacy Guidelines of the OECD. In particular there is an onus on states to justify their actions with the use of empirical evidence, how its intrusions are necessary in a particular/localised context; and additionally, how its measures are in fact the least intrusive alternative (to satisfy the proportionality requirement).
11. It is imperative that a public crisis like the current pandemic does not lead to the creation of systems to satiate a government's 'hunger for data'. Citizens and stakeholders must be afforded appropriate safeguards to ensure that they do not end up yielding their fundamental freedoms in an unlimited fashion.
12. To protect the right informational privacy we need implementable principles under a rule of law framework to guide the collection, storage, access, use, purpose and other aspects relating to people's personal information. At the same time this must be balanced with the collective imperative of ensuring people's health and safety. For this it may be useful to refer to a declaration by the Electronic Frontier Foundation (EFF) on obligations on governments to protect people's civil liberties during a public health crisis.²⁰⁵ The nature of the data collected convey very intimate details about people ranging from health status, travel histories, movements, interpersonal and community relationships, and so on.

²⁰⁵ Matthew Guariglia and Adam Schwartz, *Protecting Civil Liberties During a Public Health Crisis*, ElectroMarch 2020,

13. In this regard, governments must ensure extraordinary measures do not become permanent fixtures, which outlive this particular crisis. Justifications of government interventions in terms of necessity and proportionality must be supported with scientific evidence. It cannot be mere rhetoric and appeals to social responsibility. One example as a metric by which stakeholders may gauge proportionality is the exact time period of retention and maintenance of these data/technology systems. Specific timelines will be viewed more favourably than vague and open-ended language.
14. Considering how the coronavirus is already showing evidence of instances of discrimination against certain communities in India, it is important that data collection and processing is based on science, rather than bias. For instance, decisions should not be based on assumptions which are directly or indirectly linked with identity. To illustrate this in a real world context, consider the following example. Imagine, the Aarogya Setu application is repurposed as an e-pass platform²⁰⁶ which regulates people's movements in India. Then any decisions influenced by bias will necessarily be linked with people's fundamental rights including their right to livelihood.
15. Other essential safeguards include the need for systems to be designed towards minimal collection and deletion. Evidence of this includes a sunset clause integrated into a legal instrument, which mentions the date of expiration for any project. This must be complemented with a policy of openness and transparency with publication of detailed information about information being gathered, period of retention, tools for processing information, the manner in which all tools are linked with actual public health decision making, and the risks which may emerge through the use of these tools.
16. Finally, in order to preserve the fabric of democracies governments during public crises, is offering procedural safeguards for citizens. People must be offered avenues to challenge actions by the state in a timely and fair manner, as it builds healthy scrutiny for government actions and engenders accountability.
17. Adapting a silicon valley adage, if we move fast, we may just break more than things -- possibly, even democracy itself. It is hoped that this working paper provides policy makers in India with an opportunity to pause, reflect and consider that constitutional imperatives of personal privacy must steer technology based responses to the Covid-19 pandemic.

²⁰⁶ Maybe as an antibody/immunity certificate platform or as a mode of using public transportation