Joint Statement
on
Technical, legal, ethical and implementation concerns regarding Aarogya Setu and other apps introduced during COVID-19 in India
by
Jan Swasthya Abhiyan (JSA), Internet Freedom Foundation (IFF), Forum for Medical Ethics Society (FMES), and All India People's Science Network (AIPSN)

We, the four signatory networks of organizations of public health advocates, experts in digital privacy, science and technology policy advocates and other stakeholders issue this Statement for generating public understanding and for submission to the Government of India (GoI) and concerned Union Ministries – Ministry of Electronics and Information Technology (MEIT), and Ministry of Health and Family Welfare (MoH&FW) – about our deep concerns regarding the Aarogya Setu (AS) and other similar Apps related to the novel Corona virus epidemic. We are deeply concerned about violation of privacy, and compromised ethical principles and values, due to the AS App's design, its deployment, related policies regarding data storage, preservation of privacy and data sharing, as well as overall policy implementation and inadequate legal frameworks for data protection and grievance redressal for users.

We appreciate the need of the hour viz.:

1. the unprecedented nature and massive impact of the Covid-19 pandemic in India
2. the need for a multi-pronged approach to contain the pandemic and minimize its adverse impact on all domains of our lives
3. therefore the need for innovative approaches, including digital technology-based ones, that may be required to augment and complement other containment and mitigation measures

Key challenge

Ensuring that a balance is struck between achieving greater public good and safeguarding individuals' rights and freedoms in alignment with frameworks provided by the Constitution of India, public health ethics discourse, International Health Regulations 2005 (IHR 2005), the Siracusa Principles on Civil and Human Rights, and the Universal Declaration of Human Rights.

In this context, we conducted a detailed analysis of the AS App purposed as a catch-all solution, its Privacy Policy, Terms of Services (henceforth ToS) and Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 (henceforth, Protocol), and its code available on GitHub taking into account the broader eco-system in which Aarogya Setu has been deployed and is being used. This is presented in the more detailed position paper available with us and which informs this statement articulating key issues across five domains viz., technical and platform design; legal and policy frames; transparency and public engagement; eco-system in India in which the App has been deployed; and ethics and human rights.

Key issues

I. Technical and platform design domain

At a technical level, the AS App does not conform to key technical best practices being developed internationally. The following major concerns arise:

1. The AS App collects people's GPS trails about which many democracies, technologists and the World Health Organisation (WHO) have had concerns. It uses centralised social graph analysis to map interactions between individuals, thereby contravening the strongly supported decentralised data storage systems which safeguards citizens' real-world activities. It also uses a static Device ID which is rudimentary, and is prone to risks of re-identification (i.e. the anonymised personal data may be matched with the actual person thereby exposing who the person is).
2. The AS App's centralised data storage system enables exporting of people's sensitive personal details to an external government-operated server which is linked with the Indian Council of Medical Research (ICMR) database and others. These are being provided to third parties such as research universities and private consultancy firms. Overall, this is an expansive approach to data collection and extraction, and clearly undermines privacy of people's data.
3. The AS App categorizes people as being at high risk of COVID-19 simply based on the App's opaque algorithm and inaccurate Bluetooth and GPS based proximity tracking. This creates a non-trivial risk of false positives and negatives, leading to other severe social, personal and public health consequences. The use of self-reported symptoms also runs the risk of people wrongly marking themselves as positive or negative.

II. Legal and policy domain

1. Aarogya Setu App's privacy policy or supporting documents such as its ToS and the Protocol, assert that data retention or deletion requirements do not apply to people's data which has been "anonymised" and can therefore be seamlessly shared with third parties. This raises three key issues:
   a. standards of 'anonymization' are not defined in the ToS and the Protocol
   b. standards if any are not shared with the user and no consent sought for using their "anonymized" data
   c. there is no sunset clause for the personal data AS App collects. The, "sunset" is to the protocol rather than the underlying personal data. This evokes concerns of permanent surveillance
2. The data security and protection framework under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, are not applicable to government authorities, so there is no automatic or compulsory privacy protection
3. The voluntary Electronic Health Records Standards which provide certain privacy and security protocols for data disclosures during times of national priority, lacks suitable enforceability.
4. The latest draft of the Personal Data Protection Bill, 2019 introduced in India's Parliament in December 2019 is insufficient. It grants omnibus exemptions to Governments for emergency/ epidemic situations which is inconsistent with the contours of the right to privacy and reasonable restrictions during emergency situations as prescribed by the Supreme Court of India in its seminal right to privacy judgement in KS Puttaswamy v Union of India (2017).
5. Obligations under the IHR 2005 to which India is legally bound, require governments to ensure that national legislative frameworks relating to data sharing are adopted and be consistent with

international human rights frameworks and foundational ethical principles. Lack of such legal framework in India implies lack of protection from potential commercial surveillance.

6. From a policy perspective, there is no independent institutional oversight on (a) public agencies and the businesses developing these Apps; (b) ethical and human rights aspects; and (c) the App's actual deployment.

III. Transparency and public engagement domain

1. As per information in the public domain, Government of India (GoI), had initiated building of the AS App on March 19, 2020, and it was launched on April 2, 2020. As per standard best practice, GoI should have issued a technical whitepaper and consulted the public and external stakeholders before launching the App. However, even now, more than four months since the AS App's launch, GoI has not published any such document.
2. The lack of a structured public debate and public engagement around the AS App raises questions about its quality, and about the adequacy of ethical, procedural or institutional safeguards to mitigate risks arising from such technological interventions.
3. The National Informatics Center (NIC) has informed the media that it opted for a public-private partnership model to develop the AS App. For example, For example, UX Design at MakeMyTrip has been a private volunteer in building these systems. This evokes concerns of commercial exploitation and risk to privacy of the data collected through the AS App.
4. The underlying source code of the AS App was also not released for the longest time which is, again, best practice in such cases. Eventually, the GoI released the source code but it has not yet released the server-side code or the cloud functions. Experts have observed that the source code released on GitHub is inconsistent with the App which is being used by the public. This has therefore only marginal value in terms of transparency and is inconsistent with globally accepted standards of open source software.
5. There is ambiguity in the key AS App documents namely ToS, Protocol, and Privacy Policy. These include inadequate information for AS App users about the type and purpose of data collected, where and for how long data will be stored, with whom these data will be shared and for what purposes. A NITI Aayog official has indicated that data collected via the AS App is feeding into the development of India/Bharat Health Stack and that raises various other concerns but will not be dealt with here.
6. There is inadequate transparency about the various data points and inputs the App's algorithm relies upon to arrive at its risk scoring of users as green, yellow, orange or red.

IV. India's eco-system in which AS App is deployed

1. Indian governance systems habitually work in silos and inter-departmental coordination is extremely weak. Potential usefulness of the deployment of AS App depends upon how well the App data and its processing system is linked to contact tracing, testing and treatment through a well-equipped and trained health system. Unfortunately, there has been surprisingly little information put out so far by concerned government agencies as to how such institutional linkages have worked and how the App data has been used.

2. innovations in collection and processing of citizens' data must comply with broader legal and ethical frameworks and constitutional rights of citizens which have historically been weak and have come under increasing threat in recent times.
3. the fact that the Ministry of Home Affairs is steering this effort instead of the Ministry of Health and Family Welfare, conveys that instead of linkage with testing and treatment, the AS App is more likely being purposed as a tool for surveillance and movement control, potentially leading to social coercion.

V. Constitutional and human rights, and public health ethics

1. The Medical Council of India's Code of Ethics does not cover protocols for health data in circumstances when it is shared with the Government
2. The Government's push to make the App effectively mandatory erodes individual autonomy as guaranteed by the Constitution
3. Critically, effectively mandatory use of the AS App is inconsistent with a recent WHO guidance on ethical considerations in the use of digital proximity tracing technologies.
4. The AS App's Protocol is insufficient since it does not offer any legislative foundation for the AS App. Fundamental rights under the Constitution cannot be restricted by the Government even for legitimate purposes without express legislative authorisation.
5. Further, the Protocol fails to be consistent with standards of necessity and proportionality called for by both IHR 2005 and the Siracusa Principles. Specifically, it does not incorporate substantive language which sufficiently reigns in the government's ability to collect, store, process, retain and process people's sensitive personal details.

Our Demands: Against this backdrop, our Organizations demand as follows:

I. **For proportionality**: Three points of emphasis must be design and architecture of the AS app; transparency and effective public engagement; and limits to retention time and use of the data.

1. There is a constitutional obligation to adopt the least restrictive/intrusive measure to achieve the stated purpose. These thresholds can be benchmarked against known technological best practices and models, and the kinds of interventions adopted by other constitutional democracies. The design of interventions must also ensure that they do not disproportionately impact people from certain backgrounds, identities, and regions.
2. A full release of specifications including cryptography, anonymization specifications, Application Programming Interface (API) specifications, and Bluetooth specifications.
3. Release of the source code for the current version of the AS App, given the fact that the released code does not match with the one in use, and release of the server-side code.
4. Development of a comprehensive privacy impact assessment, articulating accompanying risks associated with large scale roll-out of the App.
5. Commitment (i.e. sunset clauses that are clearly present in primary legislation) to permanently destroy the data and systems being built via AS App at the end of the COVID-19 pandemic.
6. The AS App must not in any way be made mandatory by government or private actors;

7. Among other things, the focus must be on assuring the public that these are temporary interventions which will not devolve into permanent surveillance and monitoring systems.

II. For legality

1. Suitable legislation is required aim to hold the Union and State governments and private actors accountable for leakage or any inappropriate use of App data during epidemics and communicable disease outbreaks.
2. Under this, governments may only access patient data through hospital records, and must preserve patient anonymity.
3. These frameworks should be solely under the control of public health institutions.

III. For necessity: The government must establish:

1. The contextual necessity of the new technological interventions like the AS App which monitors people's movements since this is already being done by other actors (like telecom service providers).;
2. Grounds for treating the existing government databases, such as those maintained by ICMR and other existing surveillance mechanisms and hospital records as inadequate for the current purposes of responding to the pandemic
3. The expected advantage of interventions for collection of health and related information is collected, the actual technical effectiveness of the interventions itself, and a detailed cost-benefit/privacy impact analysis to evaluate risks before rolling out such Apps
4. Necessity as a dynamic construct, and that it is embedded through the life cycle of the AS programme. Within it there is a need for continual review of the programme as regards principles of transparency and accountability.

IV. Oversight Structures and Processes

1. The required legislation must create independent institutions for oversight separated from the political executive.
2. Towards this end, the agencies/institutions concerned should publish periodic reports informing the public if, and to what extent, the App is augmenting the Government's response in treating and containing the spread of Covid-19. Based on such feedback loops, these institutions should be empowered to make decisions for course correction or even discontinuation of the programme itself, and the permanent destruction of the systems created.