LETTER

In search of ethical pandemic technology

Published online first on June 14, 2022. DOI: 10.20529/IJME.2022.042

The duration of the pandemic over the last two years has witnessed the steering of multiple technological interventions by governments. These interventions — ranging from contact tracing applications to vaccine certificates — have been developed in the specific context of the pandemic, and were meant to address its unique requirements. This family of technological interventions may be termed "pandemic technology" — having diverse uses such as preventing the transmission of Covid-19, and aiding the relaxation of pandemic-induced restrictions. We propose a four-rung ethical paradigm for the deployment of such technology. We call it the STEP model and its four pillars consist of (i) sunset clauses, (ii) trust, (iii) equity, and (iv) privacy preservation.

While the proliferation of pandemic technology has occurred at a rapid pace, concerns remain on its largely unregulated status and inequitable uptake. The unsupervised spread of pandemic technology bears the risk of curtailing individual freedoms, and marginalising already vulnerable communities. Adopting the suggested model would therefore enable the development of privacy-preserving pandemic technology that is trustworthy and equitable, now and in future pandemics.

Essentially, the model implies that:

(i) Pandemic technology should be constrained by a mandatory sunset clause. This necessarily means that the intervention should also be backed by law. A sunset clause ensures that the law would automatically lapse after a particular date, thus de-commissioning the intervention. This is essential to ensure that intrusive emergency measures introduced during the pandemic do not spill over unjustifiably, beyond the horizon of the pandemic [1].

Designing the sunset clause contemplated above is a two-step process. Regulation must hard-code the following objects into law:

First, the clause must fix a mandatory date on which the law ceases to exist, unless extended by competent authorities. Second, the clause must contain a provision for period review, to account for any risks that the continuous deployment of pandemic technology may entail.

(ii) The deployment of pandemic technology must inspire **trust,** by checking for the following — reliability, verifiability and accuracy. Technology providing assessments of an individual's health (such as digital immunisation certificates) must be operable in both online and offline capacities, ensuring that the benefits of such technology are not lost to those without access to a smartphone or the Internet. Such technology must strive for universal interoperability, embracing open standards that can be adapted by relevant authorities for seamless access to services [2].

Ensuring trust involves communicating the scientific merits and limitations of each intervention to individuals using such technology. For example, immunisation certificates may carry a note stressing the importance of social distancing even among vaccinated individuals. This can help to avoid lowering the risk-perception of Covid-19 among people, potentially mitigating the impact of any novel variants of the virus that may emerge in the future.

(iii) The principle of **equity** must guide the deployment of pandemic technology. Here, the state must focus on equitable uptake of such technology. The state should develop strategies to overcome the digital divide prevalent in India and assume full responsibility for the uptake of such technology among the disadvantaged.

(iv) Pandemic technology must be deployed while preserving **privacy**. In the absence of a comprehensive data protection legislation in force in India, it remains critical for the state to lead with regulation that adapts universally accepted privacy principles to secure the personal data of individuals.

There is precedent that convinces us to remain optimistic on this frontier. The Aarogya Setu's Data Access and Knowledge Sharing Protocol, 2020, [3] serves as a useful regulatory example on outlining permissible uses of data collected and processed by pandemic technology. A broader framework, building on the principles outlined in this protocol can guard for privacy risks and ensure the responsible use of personal data for public health objectives.

It is important to acknowledge that the pillars of the S.T.E.P. model will robustly intersect when applied to technology. We do not view this as a limitation — interaction among the discussed principles is desirable — with each pillar nourishing the others to secure pandemic technology against misuse. The adoption of these principles could reshape attitudes towards pandemic technology, thus emboldening the perception that their just adoption forms

an integral part of our public health objectives.

Acknowledgements

The authors are grateful to Shahana Chatterjee and Siddharth Nair for their comments.

Sohini Banerjee *(sohini.chatterjee@amsshardul.com), Research Fellow, Shardul Amarchand Mangaldas & Co, Sector 41, Faridabad, Haryana 121001 INDIA;* ***KS Roshan Menon*** *(Corresponding author — roshan.menon@amsshardul.com) Research Fellow, Shardul Amarchand Mangaldas & Co, Rajouri Garden, New Delhi 110064 INDIA.*

References

1. Klar R, Lanzerath D. The ethics of COVID-19 tracking apps – challenges and voluntariness. *Research Ethics.* 2020;16(3-4):1-9. https://doi.org/10.1177%2F1747016120943622
2. World Health Organisation. Interim Guidance for Developing a Smart Vaccine Certificate. 2021 Mar19 [cited 2021 Jun 08]. Available from https://cdn.who.int/media/docs/default-source/documents/interim-guidance-svc_20210319_final.pdf?sfvrsn=b95db77d_11&download=true
3. Ministry of Electronics and Information Technology, Government of India. Aarogya Setu Data Access and Knowledge Sharing Protocol 2020 [cited 2021 Jun 12]. Available from https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf