How The Kerala - Sprinklr Controversy Represents The Gaps In India's Data Protection Framework

10/05/2020 | Bangalore

By **Aman Nair**

Edited by **Arindrajit Basu and Mira Swaminathan**

The Centre for Internet and Society, India

As COVID-19 continues to be the primary problem facing the globe, there has been a scramble among policymakers to try and utilise the latest technology in any way possible so as to contain the pandemic.Contact tracing and data analysis have become the norm, with apps to that effect being implemented world over. The Kerala government is no different, having attempted to implement similar measures by entering into a contract with US based firm Sprinklr inc. The agreement was centred around the collection and analysis of the medical details of around 1.75 lakh individuals under quarantine.
In doing so, however, it has stirred controversy and pushed numerous questions around procedural irregularities, data privacy and, subsequent effects to the foreground of the state's political discourse - even forcing the Kerala High Court to have to step in.

The importance of Privacy during a Pandemic

There is no doubt that this contract between Kerala and Sprinklr is born out of a degree of necessity. COVID-19 represents a threat, the likes of which we have not seen before. So, at the very outset, it must be asked -whether it is really worth discussing privacy implications to the potential detriment of any measure that seeks to prevent the virus from spreading through the population? Absolutely.

It is undeniably true that the government is the entity best suited to solve the current crisis facing the country. With this realization comes the inherent temptation to cede parts of individual liberty to solve the issues at hand. However any handing over of rights risks the possibility of what is seemingly temporary becoming permanent. With COVID-19 we risk entering a world wherein surveillance of individuals through contract tracing and facial recognition is normal or one where our health records exist in the public domain.
Putting aside the encroachment of the state as being reason alone, health records are an invaluable resource to corporations that may look to use the data to create targeted strategies towards a specific population. Such data can prove to be a valuable economic resource and can be used to target individuals and communities that are at their most vulnerable.

People are dying because of this virus and we must take every action to stop it. However, any measure taken to that effect must be done in such a way that it is as minimally disruptive to our rights as possible. All things considered, a balance needs to be struck between societal necessity during a pandemic and current and future privacy rights. Moreover,such a balance must be reflected in any attempt to collate and analyse health data - with such activities being done pursuant to the most stringent standards possible.

The lack of procedural oversight and exceptional circumstances in the case of Sprinklr

Moving on to Sprinklr, one of the issues arising from the affair is the apparent lack of oversight required by the government to undertake such a contract. Procedural irregularities have plagued this partnership, with the decision to adopt this agreement being taken without any involvement of the Kerala government’s Law and IT departments, which is usually a requirement for such contracts.

The government points to the nature of the pandemic and the need for a quick response time so as to save lives as justification for its acts. And yet, given that initial engagements between the parties started on 25th March and the contract was signed on 2nd April - there seems to have been adequate time to have all relevant departments be informed and have a say in the matter. Considering just how critical the data being collected was, one would hope that such vetting procedures would be followed.

What's notable however, is that for all the procedural doubts raised in front of it, the Kerala High Court - in its interim orders on the matter - made no attempt to void the contract on the basis of these irregularities, seemingly allowing for the state to adopt a 'take action and then seek forgiveness later' approach in similar situations moving forward. This represents a dangerous proposition considering the projected timescale of COVID-19, as more states may be incentivized to forgo much needed vetting and regulatory procedures due to the medical emergency.

Violation of fundamental right to privacy and lack of informed consent

Procedure aside, the fundamental issues with this deal relate to data privacy and citizen's consent. With citizens' right to privacy being affirmed by the Supreme Court in the *Puttaswamy* judgement, the state must exercise caution, and demonstrate necessity and proportionality in its collection and use of data relating to health records. To that end, following the controversy, both the Kerala Government and Sprinklr have made repeated statements outlining the steps taken to preserve data privacy of citizens, even going so far as to publish the terms of the non disclosure agreement signed between the parties.

Even so, the questions of necessity and proportionality still remain. Software systems like the one Sprinklr offers are typically used in cases wherein the volume of data to be analysed is immense. The government stance is that it was preparing for a worst case scenario that would require analysing the data of 80lakh people. Yet the fact remains that Kerala had around 1.7 lakh people in quarantine and less than 500 infected at the time of engaging with sprinklr - throwing into doubt the necessity and proportionality of Sprinklr's data analysis.

Furthermore, the High Court in its decision stipulated that any data sent to Sprinklr must be anonymised, any secondary data that has been accumulated by them must be returned and no data collected can be used by Sprinklr for commercial purposes. While this may solve the problems of this individual case, what we see is a structural failure of Indian legislation and regulations to outline minimum required standards for such contracts.

Currently there lacks a uniform agreement that the state can use across all such agreements, instead relying on contract frameworks provided for by the private enterprise And so It becomes easy to imagine a situation where states enter into multiple non uniform contracts with various organisations. In doing so there is no standardisation in terms of what exactly is owed by the corporation to the state, and the people. This could lead to different elements of an individual's data being subject to varying standards. Or even

the possibility of the same data being subject to different standards based on the corporation that has access to it.

On the question of consent, the court rightly points out the need for citizen consent in instances where their data is being handled by a third party that is not the government. Any collection of data without their consent and without the full understanding of the citizen involved would and should not be considered legitimate.

Does current necessity outweigh future difficulties - the need for closing of gaps within the proposed PDP

The ruling of the high court reaffirms what was mentioned previously,-there needs to be explicit standards outlining how to structure relationships between the state and private entities when it comes to the sharing of data. It is in view of these much needed standards, where the proposed *Personal Data Protection Bill, 2019* has a role to play. The proposed bill represents the most likely framework for data protection that India will have in the near future. The bill is meant to ensure the strike the balance between societal necessity and maintenance of individual privacy rights with regards to data. However, worryingly, under this proposed bill a number of the clarifications and protections outlined by the High Court would not be applicable.

When determining whether citizen's data can be shared with a private firm without their consent, sections12(1)(e) and 31are applicable. Section 12(1)(e) establishes that the state can process data if it fulfils the purpose of solving a medical emergency. This section therefore outlines a standard of necessity to be met, in this case a medical emergency. Section 31, however allows the government to share any collected data with a third party, however without any need to meet a standard of necessity. . To be clear, this means that the necessity relates to the processing of the data, with no standard of necessity required for the transfer. A ministry or department would therefore, having met the standard for necessity in terms of processing, not have to make any justification for their outsourcing of data to a private firm. More worryingly, there is no set of regulations on what type of firm can have the data shared with it or any minimum standards that must be met for the government to choose an entity to process its data. In terms of sharing data with a foreign entity, there is no standard of necessity, once again. The only stipulation that must be met is that any data transferred must remain stored within India.

However, the single biggest deviation between the protections provided for by the High Court and the PDP bill comes down to the anonymisation of data. While the court mandated all data transferred to the foreign entity be anonymised, no such provision exists within the PDP. The bill fails to place a requirement on either the government (fiduciary) or the private entity (processor) to anonymise any data it receives. This opens a multitude of problems given the sensitive nature of the data and how such data can be used in the future.

Furthermore the current bill places no statutory liability on the processor. Rather it places all liability solely upon the government and as such any legal action taken by an individual to protect their data must

be taken up against the state and not the private entity. This means that entities such as Sprinklr may not be directly accountable to citizens despite having access to their data, but are rather liable only to the extent of their contract with the government.

Conclusion

Ultimately what is clear is that while the individual grievances in the case of Sprinklr have seemingly been addressed by the High Court, there are glaring gaps between what should be done, what has been recommended and what will most likely be law in the future. The court stressed the point of "ensuring that there is no data epidemic after the COVID-19 epidemic is controlled", however with the current gaps in India's data protection framework it is likely we will see such a "data epidemic" long after COVID-19 is controlled.