Sprinklr: Avoid Data Epidemic

1. Introduction

So much has been written in recent times on the inadequacy of Indian data protection law, particularly the proposed Personal Data Protection Bill of 2019 (**"PDP Bill"**). Privacy in India is a nascent concept, validated by the Supreme Court that expanded Article 21 of the Constitution and recognized it as a fundamental right in *Justice K.S Puttaswamy (Retd.) & Anr. V. UOI.* The Supreme Court stated that like most other fundamental rights, the right to privacy is also subject to various checks and balances, including reasonable restrictions. In other words, to ensure that the fundamental rights remain sacrosanct and are not infringed, the settled judicial position is that there should be a legitimate aim of the state versus arbitrary actions and the restrictions of any intended law must be "reasonable."[1] Recently, the state government of Kerala came under intense judicial scrutiny (and political controversy) for engaging an American company to manage the data of its COVID-19 patients.

This newsletter discusses the case of *Balu Gopalakrishnan & Anr v. State of Kerala and ors.* and its contribution in the ongoing privacy debate, particularly when dealing with sensitive personal data relating to health.

2. The Facts, Arguments & Order

The state government of Kerala executed a contract with Sprinklr Inc., a US software company, through which the latter created an online digital platform to process and analyze data pertaining to COVID-19 patients and those susceptible to it, in the state. The state collected data of such individuals and uploaded on Sprinklr's servers. Sprinklr was to analyse the data and provide its inputs with the analyzed data to enable the government to handle the virus. Concerns arose and were expressed that by assigning health data to an American company the privacy of patients and quarantined persons was at risk, more so in the absence of safeguards against potential commercial and unauthorized exploitation of the data by Sprinklr. The Kerala High Court had to determine if the contract contained enough safeguards to ensure confidentiality of the data collected and the mode of dealing with it, after analyzing it.

2.1 *Petitioner's Position:* The petitioner questioned the need of the state government to go overseas to engage an entity for storing sensitive data when state-owned agencies were equipped could well undertake the task. Amongst other points, it pointed out **(a)** the state should obtain the consent of the persons whose date was collected; **(b)** the safety of sensitive personal information of Indians collected and stored by Sprinklr was questionable and it would be necessary to consider if it can exploit such data for commercial gain; **(c)** the contract was executed without following due process, was in conflict with Article 299 of the Indian Constitution[2] and qualified as a misuse of the arbitrary power of the State; and **(d)** in the event of a dispute including breach of confidentiality, the contractual recourse was to seek a remedy in the courts of New York. By agreeing to a foreign

[1] The obvious instances include national security, crime prevention, innovation
[2] Article 299 (1) requires that all contracts made in the exercise of the executive power of a state must be executed by the Governor or someone he authorizes

jurisdiction, the state had made it very tough for affected persons to seek appropriate judicial remedies in the event of a breach.

2.2 *Respondents Position:* The state submitted that due to the rise in the number of COVID-19 cases **(a)** there was a dire need to incorporate tracking and tracing mechanism to collect health related data and engage a credible entity, capable to handle and store such sensitive information. The state government entities did not possess the technical ability to manage voluminous data. Therefore, there was a need to go offshore with a company that possessed both capacity and infrastructure to manage the data; **(b)** it firmly believed that the confidentiality of data was guaranteed under the contractual terms and the government shall be fully responsible qua such persons; **(c)** given the urgency, the state executed a standard form contract with Sprinklr which granted exclusive jurisdiction to courts in New York, but as the data was retained in India any breach of its confidentiality would be actionable. And, they would anonymize all personal data before it is disclosed to Sprinklr.

The second respondent, Union of India, took the position that their primary concern was on citizens data confidentiality which should be preserved at all cost and should never be breached. It felt the contract did not contain enough safeguards to protect confidentiality. Moreover, it was of the view that India possessed ample competence and there was no need to go offshore or risk judicial recourse to foreign courts, with the possibility of an elusive outcome. From the arguments put forth by the parties, it is evident that the Indian government wishes to treat sensitive data of individuals in a way that a copy of all sensitive personal data is required to be stored in India.

2.3 *Court's Order:* Upon hearing the parties, the division bench of the high court admitted the petitions and restrained Sprinklr from **(a)** committing any act which will, directly or indirectly, be in breach of confidentiality of data and disclosing such data to any third party; **(b)** advertising or representing to any third party that they possess or have access to such sensitive medical data of patients or potential patients; **(c)** using or exploiting the data, or the name and emblem of the state government, directly or indirectly, for any commercial benefit. Expressing concern over the confidentiality of information gathered from the patients, it additionally directed the government to:

- anonymize all sensitive personal data collected in the past and to be collected from citizens before allowing Sprinklr to access such data;
- inform all citizens that their collected data is likely to be accessed by Sprinklr or other third-party service providers, and obtain their specific consent to such effect
- ensure that the data is returned to the state upon completion of contractual obligations.

Clearly, the focus of the court was solely to prevent breach of confidentiality, which means protecting it from unlawful, unauthorized and unintentional access and disclosure with appropriate limits on those who could view, use, analyze and have the potential to disseminate and share that data. Consequently, the criteria for data disclosure, handling or processing require ample checks in order to protect confidentiality. The court had taken the position that the contractual safeguards were insufficient against breaches of data confidentiality. At the same time, it had to strike the balance and noted that it did not think it prudent to issue orders that would impede the efforts of the state in fighting the pandemic.

Subsequently, on May 18, 2020 the state released a circular with 11-point guidelines to be followed in the collection transmission, storage or processing of Covid-19 related personal

information of citizens. This circular is based on the court directions and principles outlined in the foregoing bullet points on anonymization and consent. Further, in the context of data storage it provides that where possible, data is to be stored in an encrypted form in the state data center. If stored on cloud, then the service provider has to be approved by Indian government and prescribed guidelines of different departments for procuring cloud have to be followed too. For using a third-party system, it should be ISO 27000 enabled. The foregoing mandates of the court will have to be followed strictly and, in addition, those contracting with Kerala state government agencies processing COVID-19 data, shall have to conform with the prescriptions of the guidelines as well.

3. The Debate Continues: Necessity, Privacy & Safeguards

It is necessary to evaluate this important judgment in light of the existing and even the proposed legal framework surrounding data protection in India. While the High Court took the correct step and mandated that the data be anonymized before it is provided to Sprinklr, but no standards of anonymization exist currently. The present law is contained in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011. And, these obsolete rules are silent on how corporations should deal with anonymized data. Further, there is no settled jurisprudence either that prescribes the framework on anonymity, but with increasing digitization it is now an integral part of the rights of an individual. Section 3(2) of the draft PDP Bill defines "anonymization" in relation to personal data as "*such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standard of irreversibility specified by the Authority.*" So, once the PDP Bill becomes law and the Data Protection Authority is established thereunder, it should prioritize in prescribing standards of de-identification whereby key identifiers associated with an individual are removed and it is not possible to identify such person. The use of the word "irreversibility" in the aforesaid section seems to suggest that stringent standards will and ought to be used and applied.

There are divergent views on whether anonymized data is totally anonymous since there can be means to reidentify individuals, through multiple data points combined with the aid of other tools, which can pose a serious threat to privacy in health matters. While we shall not get into that discussion, the requirement for anonymization of user data does is critical and cannot be over-emphasized, more so in the absence of adequate statutory protections. In recent months the pandemic and consequential lockdowns have led to a spurt in the growth of telemedicine. And, at a such time the need for applying highest care to patient data should be non-negotiable, more so when analysts are mapping behavior on the basis of profiling individuals and examining their footprint across different online forums, social media or otherwise. While sharing data is, perhaps, essential to find a cure and for governments to map the virus, but this cannot come at the cost of compromise on individual privacy or without express consent. Even the court stipulated that informed consent and notice be obtained from users for the data transfer where identifiable personal data is disclosed. Where such collected personal data is anonymized and then disclosed, there is a divergence of opinion on the legal obligation to obtain consent in relation to its disclosure.

Rapid recourse to judicial remedies is again integral to protection of individuals in the event of breaches. As noted, the Sprinklr contract provided that should a dispute occur including breach of confidentiality, the contractual recourse was to seek a remedy in the courts of New York. The overall sentiment was that the state made it very tough for affected persons to seek appropriate judicial remedies. Usually, if a party decides to apply to a court for relief, be it a state or an individual, efficaciousness and speed are paramount concerns. India and the US do not have a reciprocal arrangement for enforcement of their respective court orders. Therefore, overriding practical

difficulties in the enforcement process can be a challenge when the contract is between resident and non-resident parties. Getting embroiled in a protracted battle is not optimal for the relevant parties. Perhaps, given the stakes involved plus the permutations and cross-roads of sensitivity of data, coupled with overarching privacy concerns, it may be more prudent plus effective to consider and opt for mediation as a dispute resolution remedy. This, obviously, requires the ability of the disputing parties to set aside vested interests and look at the larger picture, particularly in the context of a virus.

Subsequently, on the basis of an affidavit submitted in court, the state government stated that **(a)** database covering COVID-19 patients and those being monitored was transferred to the government-owned cloud web space.[3] Once this transfer was implemented, no data was sent to Sprinklr; **(b)** it asked Sprinklr to destroy all residual data immediately; **(c)** in order to send future data to Sprinklr, amongst other things, anonymization would be followed.

4. Conclusion

There is no question the pandemic has been the biggest global challenge witnessed in the last 100 years and, the lack of knowledge on the subject, has led to different nations taking different steps to detect, monitor, trace and contain the virus. Six months into the pandemic, global partnerships continue to be relevant. While Indian companies may possess the ability to do excellent and necessary data analysis, but the need for massive infrastructure combined with the required technical capabilities and with ability to scale up rapidly cannot be undermined and, to that extent, perhaps, the intent of Kerala (or any state) government to go offshore should not be politicized or not be considered an optimal solution. At the same time, the balancing interest have to be considered and evaluated at each step, be it of the state to manage a health emergency or of an individual whose privacy should be preserved. In the course of the proceedings, the court had stated they intended *"to ensure that there was no "data epidemic" after the Covid-19 epidemic is controlled."* In summation, handling the pandemic in the most efficient manner is in the interest of all BUT with necessary safeguards to protect the data and minimize the risks which could arise from its usage and avert the likelihood of a future "data epidemic." To this end, the interim orders in the Sprinklr case are a step in the right direction.

Author
Priti Suri

The views expressed are personal to the author

[3] This space is managed and controlled by C-DIT or the Imaging Technology Development Center. The government had asked Kerala State IT Mission and C-DIT to ensure that all the data collected was anonymized before transmitting to any third-party service provider or using in conjunction with any software for data processing