Is Privacy an Illusion for the Netizens of the 21st Century?

Image source: yourstory.com

Anjali Sunil

Innovation is considered to be the fuel of the 21st century. Technologists all around the world are constantly creating systems that can be used in making corporations and governing systems more efficient. This includes surveillance systems used to effectively monitor public ecosystems to protect citizens from crimes and control them in times of pandemic. An extensive use of data has been more pronounced in recent times to enforce strict quarantine measures in combating COVID-19. However, this is bestowing more power on the government to monitor its citizens and the lack of comprehensive laws to regulate such power is really concerning. We are still governed by some archaic laws, which combined with the technological prowess of today become a lethal combination for privacy.

Privacy post-Puttaswamy

India, which has become a country with the largest database of biometric data by adopting the Aadhaar Act, is prone to exploitation and malpractices. The recent developments have further amplified India's vulnerability to data breaches. In 2017, the Supreme Court in *Puttaswamy vs Union of India* unanimously held the Right to Privacy as a fundamental right under the Article 21 of the Constitution of India, which states "No person shall be deprived of his life or personal liberty except according to the procedure established by law". The judgment laid out tests limiting the discretion of the State in processing data. It includes the following doctrines.

i. Legitimacy: The action must be sanctioned by the law to justify an encroachment of privacy.
ii. Necessity: The proposed action must be necessary in a democratic society if there is a compelling State interest.
iii. Proportionality: State's exercise should not have a disproportionate impact on the right of the individual. There should be a direct balance between the identified goal and the method used to achieve it.

The surveillance technology used in handling the ongoing pandemic has to satisfy these tests. It is essential to guarantee that the basic human rights are not abused in the quest for securing national interest. The pandemic has unveiled a rather disturbing trend across the Indian States where the privacy of individuals has been violated in the bid to contain the disease spread. Technology has been deployed at three levels. First, in creating a list of persons suspected to be infected with COVID-19; second, in

deploying geo-fencing and drone imagery to monitor compliance by quarantined individuals; and third, through the use of contact-tracing smartphone applications such as Aarogya Setu.

In Kerala, apps that use geofencing are being increasingly deployed. Geofencing is a location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location to monitor quarantined citizens. A similar measure taken in Karnataka includes uploading a selfie every half an hour. The 'selfie' itself is geotagged and would be verified for its real-time nature. This means that the State department is collecting real-time information compulsorily without any comprehensive law stating its proper disposal, considering the sensitive nature. Other states such as Telangana and large municipalities like the Brihanmumbai Municipal Corporation (BMC) use geotagging features to steadily monitor strict enforcement of the lockdown. State governments such as Chandigarh, Delhi and Karnataka purportedly transferred quarantined individuals' list through WhatsApp and other social media platforms. Recently, the district administration of Mohali followed the suit and published personal information of COVID patients in the public domain, violating the privacy of the individuals who had submitted the data in good faith to the government.

There may entail a compelling justification to override individual privacy to tackle a health crisis of this magnitude. However, such disclosures have a devastating impact on individual liberty, which is manifested in the form of stigma generated against those undergoing quarantine and those at the frontline. As reported by *the Hindu* on April 20, 2020, "If reporting symptoms would cause personal data to be shared on the public domain, it will deter the public from coming forward at a time we desperately need their cooperation". While there exists a legitimate state of interest for the rigorous use of data to halt the spread of virus, it cannot violate the basic rights guaranteed by the Indian Constitution.

Test Compliance

In the three areas of technology deployment, a question arises whether the government has satisfied all the tests mentioned in the Puttaswamy judgment. Although the collection of data of people suffering from COVID-19 satisfies necessity as channel through the Epidemic Diseases Act of 1897, the publication of such data on public platforms has led to increased stigmatisation and problems, thus violating principles of proportionality, as the State should achieve its aim of pandemic containment without compromising on the privacy of citizens infected and leading to alienation of individuals and families. The usage of Aarogya Setu particularly raises many concerns. An astonishing parallel can be drawn with the Aadhaar Act, which gives discerning information to the government without an established legislation regulating it. It fails the test of legitimacy.

In recent developments, the government officials have indicated that train passengers and air travellers have to mandatorily install the Aarogya Setu app before boarding. There is an existing mandate for the government employees to download the app. The reported coercion of downloading violates the concept of voluntary dissemination of information as upheld by the Right to Privacy Act, without establishing a sound State aim. While the principle of necessity can be satisfied as pandemic control is a necessary step towards its successful elimination, the doctrine of proportionality seems questionably unsatisfied. The terms and conditions of the app enunciates that the Government of India will not be liable for any unauthorised access

to citizens' information or modification thereof. This acquits the government of its liability, in case there is any leakage of information.

As we can see, the pandemic containment measures of the government using technology are not satisfactory of the existing legislations, and the absence of a data protection bill grants limitless powers to the government. Although necessity stands unquestioned, there is little evidence to prove that the doctrine of proportionality is satisfied. Thus, unfolding the legislations stands in violation of the Constitution. Inter arma silent leges, said Cicero: "For among [times of] arms, the laws fall mute". However, the laws were not authored only during times of peaceful cohabitation, they were meant to be followed during crises as well.

This leads to a very important question that frames the core of the privacy debate in India: "Should governments have access to sensitive data which they can utilise for an infinite period of time without accountability?" The crux of the issue is that despite privacy being recognised as a fundamental right, the existing legal provisions give several outlets to override the privacy concerns of the public.

Legal Landscape

India, at present, does not have an explicit legislation governing data privacy. The pertinent law dealing with data protection is the Information Technology (IT) Act, 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) rules, enacted under Section 43A of the Information Technology (IT) Act, 2000. The Act covers privacy provisions in narrow constraints where a concept like personal data and consent are not defined. This makes privacy a mere illusion.

Similarly, other laws such as The Indian Telegraph Act, 1885 (Section 5), empowers the Central Government and the State Government to order the interception of messages in two circumstances: (1) in the occurrence of any "public emergency" or in the interest of "public safety", and (2) if it is considered necessary or expedient to do so, in addition to the following instances: in the interests of the sovereignty and integrity of India; the security of the State; friendly relations with foreign states; public order; and for the prevention of incitement to the commission of an offence. However, the IT Act does not have this overarching condition, which means information can be decrypted and monitored even in cases where there is no public emergency as the conditions are vague.

The Personal Data Protection (PDP) Bill of 2019 attempts to address some of these concerns. However, the much-anticipated Bill in its present form has many lacunae. As per Section (36) of Chapter 1 of the PDP Bill, Sensitive Personal data has been defined as having the attributes of financial, genetic, sexual, biometric, religious and caste affiliation, etc. This Bill separates very sensitive personal data from personal data, which has been referred to as the markers of identification of an individual made available in the public domain. However, the Clause 12 (b) of Chapter 3, which states "Notwithstanding anything contained in section 11, the personal data may be processed if such processing is **necessary** under any law for the time being in force made by the Parliament or any State Legislature", allows governments to process data as per any existing law or regulation already adopted in the Parliament. This means that the government

has the power, under the IT Act, 2000 Section 69A and 69B, to control the dissemination of information, and monitor and collect information.

The Bill gives an exit clause for the existing laws to continue functioning, and it did not seek to address the lacunae of the IT Act. It only replaces a clause in Section 43A and Section 72A of the IT Act to the extent of victim compensation, thus leaving a lot of loopholes for the misuse of sensitive data.

Sections 13 and 14 of Chapter 3 of the Bill bestows power on corporate bodies to access personal data of employees without their consent. The very fact that while collecting data it is not segregated into highly sensitive and sensitive data, and measures not taken to address it poses a grave problem that can manifest in the form of prejudice and discrimination. Additionally, the condition on non-consensual processing of data fulfils the *necessity* criteria only. Processing of non-consensual data should not only be on the basis of necessity but also on the basis of proportionality to the need.

There is an exigency to reconsider the data collection methods to provide higher security for sensitive data of the Data Principal[1]. The Data Fiduciary[2] can access the data available in the non-sensitive personal data category for provision of services, but the law needs to strictly enumerate these conditions and replace vague rules that are subject to varied interpretations. Similarly, given the fact that data is available in the public domain does not make it non-sensitive in nature. Thus, care should be taken to provide adequate protection to the data irrespective of its availability status.

As India is increasingly relying on the use of data to drive its decisions, it is important that the laws within which these data systems operate are equipped with safeguarding the interest of the data subjects. The surveillance technologies used in combating the pandemic should be consistent with the threefold tests laid out by the Puttaswamy judgment, where the extent of interference should be authorised by law and must be proportionate to its need.

Anjali Sunil is Research Intern at Centre for Public Policy Research. Views expressed are personal and need not reflect or represent the views of Centre for Public Policy Research.

References

1. "Data Protected India: Insights." (n.d.). Accessed 20 April 2020. https://www.linklaters.com/en/insights/data-protected/data-protected---india.
2. "Data Protection and Privacy Issues in India." 2017. Economic Law Solicitors [PDF File]. Accessed 20 April 2020. https://www.sci.gov.in/pdf/JUD_3.pdf.

[1]"Data principal" means the natural person to whom the personal data relates to.
[2]"Data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

3. Flaherty, H. David. 1991. "On the Utility of Constitutional Rights to Privacy and Data Protection." *Case Western Reserve Law Review* 41: 831. Accessed 20 April 2020. https://scholarlycommons.law.case.edu/caselrev/vol41/iss3/14.
4. "GDPR-loving EU says India's Data Localisation Unnecessary." 2018. *Economic Times*, November 21. Accessed 20 April 2020. https://economictimes.indiatimes.com/tech/internet/gdpr-loving-eu-says-indias-data-localisation-unnecessary/articleshow/66725579.cms?from=mdr.
5. Kumar, S., and Bhardwaj, S. 2020. "The Publication of COVID-19 Quarantine Lists Violates the Right to Privacy." *The Caravan*, April 5. Accessed 20 April 2020. https://caravanmagazine.in/commentary/covid-19-pandemic-quarantine-lists-right-to-privacy.
6. Laws and Guidelines referred include: Personal Data Protection Bill, 2019; The Indian Telegraph Act, 1885; Information Technology Act, 2000; Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information Rules, 2011; Public Records Act, 1993; The Aircraft Act of 1934; General Data Protection Agreement (European Union - GDPR); Mutual Legal Assistance Treaties (MLATs); Fundamental Right to Privacy Judgment Document; Article 17, 19, 20 and 21 of the Indian Constitution.
7. PricewaterhouseCoopers. (n. d.). "Data Localisation Norms: A Key Pillar for Privacy Protection." Accessed 20 April 2020. https://www.pwc.in/consulting/cyber-security/data-privacy/data-localisation-norms.html#sources.