Right to privacy: Recognising data protection as a fundamental right

July 2020
On 24 August 2017, the Supreme Court recognised privacy as a fundamental right in a landmark judgement delivered in Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. The nine-judge bench of the apex court unanimously observed that privacy is a protected constitutional right under Articles 14, 19 and 21 of the Constitution of India. It also considered privacy as a basic human right and an integral part of human existence. In most countries, privacy is either protected as a constitutional right or by data privacy legislation which considers privacy to be a fundamental human right.

The discussion on recognising privacy as a fundamental right can be traced back to the 1950s. In the 1954 judgement by the Supreme Court in the case of M. P. Sharma vs. Satish Chandra, in which the constitutionality of search and seizure of documents from a person against whom a first information report (FIR) has been filed was challenged citing that such procedures violated Articles 19 (freedom of speech and expression) and 20 (right against self-incrimination), an eight-judge bench held that the drafters of the Constitution did not intend the power of search and seizure to be violative of privacy. The bench found that the concept of a fundamental right could not be applied to privacy in cases of search and seizure as such processes were temporary and did not require statutory recognition.

The recognition of privacy as a fundamental right allows every Indian to approach any high court (under Article 226) and the Supreme Court (under Article 32) to seek judicial remedies.

As the 2017 judgement observed, “Dignity cannot exist without privacy. Both reside within the inalienable values of life, liberty and freedom which the Constitution has recognised. Privacy is the ultimate expression of the sanctity of the individual.” While recognising privacy as a fundamental right, the apex court also stated that it must be in accordance with the law. This observation is in agreement with Article 21, which states the following: “No person shall be deprived of his life or personal liberty except according to procedure established by law.” The apex court believes that the right to privacy must meet the threefold requirements of (i) legal meaning as per the prevalent law in India, (ii) the need for a legitimate aim and (iii) proportionality (i.e. the rationale between the purpose and the means deployed to achieve it), and such restrictions are applicable to both citizens and the state alike.

The judgement has paved the way for establishing a privacy law in India, especially for informational privacy. It also casts obligations on corporations and organisations to prioritise and undertake utmost care to secure and respect personal data collection and usage.

### Implications for organisations in India

If we look at the draft Personal Data Protection (PDP) Bill, 2019, from the perspective of the judgement on privacy, it becomes clear that organisations are to abide by concepts like responsibility, accountability and choice when they are dealing with an individual’s data.

Any data processing activity undertaken in India by government/private organisations or individuals should be in accordance with the principles mentioned below.

- **Definition of personal data and its protection:** As per the Supreme Court’s observation, any information that is private in nature can be termed as personal information and comes within the purview of privacy protection. Various examples in the judgement imply that certain personal information holds a higher risk value when it comes to causing harm to individuals and can be classified as sensitive. For example, information about sexual orientation or an individual’s health records (which may impact an individual’s reputation or dignity) demand a higher degree of protection and care.

- **De-identification of personal data wherever possible:** Any personal information that is anonymised and de-identified using de-identification techniques remains out of the scope of misuse and consequent legal action for organisations. Organisations should invest more in de-identifying tools and technologies to anonymise data collected by them.

---

1. Justice K.S.Puttaswamy (Retd) & Ors vs Union Of India & Ors, WP (C) 494 of 2012, Judgement dated 24th August 2017
3. Justice K.S.Puttaswamy (Retd) & Ors vs Union Of India & Ors, WP (C) 494 of 2012, Judgement dated 24th August 2017
• Ability to exercise choice: Consent of individuals is of utmost importance when it comes to data processing and must be taken explicitly before collecting and processing personal data. The data processing activity should be just, fair and reasonable – especially when related for commercial reasons. Transparency should be considered as the basic principle when it comes to dealing with personal information.

• Process data only if/when necessary: The draft PDP Bill states that a data processing activity should only be carried out when the data collected is proportional to the purpose for which it is being collected, with a legal and fair objective. Thus, organisations need to clearly analyse each individual activity which results in collection of personal data to ensure that a legal basis is identified and recognised.

• Provision for the ‘right to be forgotten’: Every individual must be given the option to delete her/his personal data as people change and evolve over time and so do their choices. To be able to track a person’s activities or attempt to predict her/his future actions exclusively on data collected from them in the past could cause immense harm to an individual.

• Respect the individual’s ownership of her/his own data: The Supreme Court observed that a person has the right to protect collected personal data from unwanted access. Thus, companies should embed procedural and technical capabilities within their environment to ensure that people can assert certain rights on data collected from them.

• Incorporate privacy checks in audits: Data processing activities by both government and private bodies are subject to the tests of proportionality and legitimacy. These should be the basic parameters to be considered from a privacy perspective when data is being audited.

• Implement a privacy risk assessment process: The procedures put in place for personal data processing should be evaluated against the risks involved and benefits derived from them. Privacy should never be a ‘price’ an individual has to pay for either availing services or convenience, unless such services fall under the categories of research, public welfare, analysis of epidemics, criminal investigations, national security, etc. This also signifies the importance of data privacy impact assessments and privacy by design concepts to be conducted and implemented by the bodies processing private data.

• Exercise caution while profiling: An individual expects a level of privacy and harm to be managed in every data processing activity. Thus, profiling activities should be restricted, conducted with caution and have space for manual intervention. Care should be taken to ensure that identities of those from whom data has been collected are protected and proper checks and balances are in place.

• Develop a privacy by design culture: The Supreme Court observed that in certain cases, even consent fails to safeguard the privacy of an individual. Hence, organisations collecting data should ensure that adequate controls are built in from the beginning and in a proactive manner to cover the entire data lifecycle, from collection to deletion.

The views expressed by the apex court strengthen the need to treat the privacy of individuals more seriously and contextually. Government and private organisations can no longer afford to be unconcerned about the personal data collected by them. They must take ownership of such data and make sure that the checks and balances built around accountability, rights of users, transparency and purpose are applicable equally to public and private sectors.

The Supreme Court’s judgement paves the way to frame newer rights around areas of surveillance, online sales and marketing, ownership of personal data, the extent of profiling human and genetic traits, etc., in the future.
Contact us

Dhritimaan Shukla
Partner and Privacy Leader
PwC India
Mobile: +91 98990 38326
dhritimaan.shukla@pwc.com

Sonali Saraswat
Associate Director, Privacy
PwC India
Mobile: +91 96207 01515
sonali.saraswat@pwc.com

This article has been researched and authored by Sonali Saraswat, Debasree Mukherjee and Dhritimaan Shukla.
The views expressed in this article are personal opinions of the authors and should not be construed as legal interpretation.