

**INTERNATIONAL JOURNAL OF LAW  
MANAGEMENT & HUMANITIES**

**[ISSN 2581-5369]**

---

**Volume 4 | Issue 3**

**2021**

© 2021 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

---

This Article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

To submit your Manuscript for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Need of Privacy Law in India

---

ANJALI KUMARI<sup>1</sup>

## ABSTRACT

*As this article highlights about the problems arising from the New Whatsapp Privacy Policy and the need for data protection law in India. Privacy can be understood as a right of an individual to decide who can get right of entry to the data, when they can get entry to the data, what data they can get entry to. Indian constitution defines Privacy as personal liberty in Article 21. "Protection of Life And Personal Liberty" No individual shall be deprived of his life or personal liberty except according to the process established through law. The notification was made 'after' the WhatsApp New Policy, which states that it may share data of any of its users with its own circle of relatives of companies (Facebook). This new update has prompted numerous difficulties over the privacy of the people that use this application. The new policy permits Facebook to get entry to these business interactions and user purchasing interest to target advertisements and customize content. WhatsApp/Facebook cannot see the user's personal messages, group messages, or listen calls with their friends, family, and co-workers, due to the fact it is protected by end-to-end encryption.*

**Keywords:** Article-21, Privacy Policy, Data Protection, Whatsapp, Personal Liberty.

The **Personal Data Protection Bill, 2019**, follows an extended line of privacy jurisprudence in India that has been encouraged by worldwide developments in addition to the country's personal constitutional jurisprudence. Though the constitution does not explicitly point out a right to privacy, Indian courts have held that a right to privacy exists under the right to life assured under Article 21. The bill aims to protect the informational privacy of individuals by developing a preventive framework that regulates how businesses acquire and use personal data, instead of protecting informational privacy with a purpose to the resultant harm due to the violation of such privacy. In doing so, it focuses generally on regulating practices related to the usage of data.

The debate on the privacy concerns, Why India needs to take data privacy seriously? Data confidentiality and privacy is a primary right which Indian customers need to demand, because the economic system turns into more and more digitally pushed. Data privacy and protection

---

<sup>1</sup> Author is a Student at Lloyd Law College, India.

is a fundamental basis for a rising data-driven economy like India. Permission advertising and marketing will be the subsequent battleground manufacturers or entrepreneurs will need to take cognisance of, as India transforms from a data-poor economy to a data-rich economy.

At the ultimate count, India has claimed the first region in the world with 270 million Facebook users accompanied by the United States which has 240 million Facebook users. Indians are leaving at the back of so much personal data and information on this social media platform which is available to the world. Poor data protection tradition in India. In the past, little or no interest has been paid in India to personal data and privacy. It's not unusual for customers right here to share their personal information with distinct companies and entities – PAN card, Aadhaar card, mobile number, email id, address, phone numbers – are effortlessly doled out. Personal data is continuously misused by distinct companies or service providers. Data robbery or selling data is very common however it needs to stop. When a data breach happens, the business, entity or individual liable for the breach should be penalised.

Data confidentiality and privacy is a primary right. Indian customers need to learn how to exercise this right because the economy turns into digitally driven.

- Often, a commercial enterprise does not take consent of the consumer before the usage of personal data. The definition of valid consent in the Indian jurisdiction then turns into very important.
- Collection – There needs to be readability on why data is being collected, for what purpose, and requires clean articulation. Nowadays, plenty of data is asked by distinct companies or entities in the enrollment or purchase form, invoices and bills or when while registering for online subscription.

However, its purpose is not defined. Permission to procedure – It is essential to provide the customer a right to persuade or provide permission to process the data. Also, they have to be allowed to provide or withdraw the right to companies to rectify, add or get right of entry to this data. To get admission to any form of personal data, collection, entry to, permission to apply this information by distinct companies need to be made mandatory by a data regulator or a data protection authority. Also, a clear data protection law will make sure that each time there's a handshake of Personal Identifiable Information by companies for numerous reasons throughout channels and service providers, confidentiality and therefore privacy is maintained.

As India receives data mature over the years, a clear enforcement version will be necessary, in the course of a breach of personal data. Setting requirements, privacy exchange platform and tracking data turns into important and there will be a massive need to enhance attention

amongst Indian customers and businesses. Non-compliance and misuse of personal data and breach of privacy should appeal to strong penalties. Data protection and privacy act with common requirements throughout the country to protect the fundamental right to privacy of each Indian will move a long way.

These issues recommend a need for an extra pragmatic and modest method to protect data and harm from misuse of personal data. Since the bill treats privacy as an end, the proposed framework is preventive, all-encompassing, and incredibly regulated. In doing so, it considerably strengthens the strength of the state to regulate entities that accumulate data and gives the state additional levers to behavior surveillance. There are apparent limits to the efficacy of protecting privacy through this regulatory design. Instead, the framework must narrowly and exactly recognize issues that can be meaningfully addressed through regulation. The following factors enumerate the possible components of this kind of framework:

- Data should not be collected and processed without consent.
- The remaining preventive regulatory duties should be layered, based on an evaluation of their costs and benefits.
- Regulatory uncertainty needs to be reduced.
- The power given to the government to exempt any government agency from the requirements of the bill should be balanced with adequate safeguards enumerated in the bill itself.
- The mandate given to the DPA should be cognizant of state capacity constraints in India.
- The DPA and the government should comply with a highly consultative process for decision making.
- Lastly, since the functioning of the DPA has an essential bearing on the market, its composition should enable it to avail of unbiased inputs in an institutional manner.

As this article discussed, the regulatory framework proposed for protecting the privacy of citizens needs to be definitely tailored for the realities of the Indian economy and its regulatory landscape. It is essential to have a realistic approach to data protection. In the characterization of privacy as an end instead of a means to protect different important societal ends that are particular to India's political economy, the bill substantially strengthens the state without properly protecting privacy. Designing a more specific and pragmatic regulatory framework can only be carried out through a practical evaluation of the costs and advantages of data protection for India.

**REFERENCES:**

- <http://www.legalserviceindia.com/legal/article-3371-why-data-protection-bill-2019-is-important-for-india.html>
- <https://www.dw.com/en/indias-personal-data-privacy-law-triggers-surveillance-fears/a-55564949>
- <https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india-everything-you-must-know>
- <https://www.legal500.com/developments/thought-leadership/personal-data-protectionlaw-in-india/>
- [https://m.economictimes.com/tech/technology/after-facing-backlash-whatsapp-clarifies-its-new-privacy-policy/amp\\_articleshow/80226028.cm](https://m.economictimes.com/tech/technology/after-facing-backlash-whatsapp-clarifies-its-new-privacy-policy/amp_articleshow/80226028.cm)
- Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?  
Anirudh Burman

\*\*\*\*\*