The Cambridge Dictionary defines privacy as ‘a state in which one is not observed or disturbed by other people’. For example, one has a right to sleep in his/her house unwatched and undisturbed. Secrecy is defined as possessing information that can potentially have a negative impact on someone else – either emotionally, physically, or financially. It is believed that the disclosure of confidential information has the potential to harm people. For example, trade secrets and confidential company data are often considered as classified information. Thus, privacy is sometimes erroneously considered to be synonymous with ‘secrecy’.

**Decoding privacy for different people:** Privacy is essentially a psychological concept about creating boundaries and can be interpreted differently by individuals. It is largely about the ability to choose how to disclose information, whom to disclose it to, how much is to be disclosed, and identifying the purpose of the disclosure. The decision to disclose any information and the extent of disclosure depends on what are the perceived ‘risks and benefits’ for the information in consideration. This means the extent of disclosure will be dependent on the culture, region, context, expression and the ability to control the dissemination of said information.

Historically, India has been a collectivist society with a low individualism index. Indian culture has revolved around joint families and a strong sense of community, where an individual’s business is everyone’s business, thus lowering the importance attached to privacy. The concept of privacy in India largely continues to circle around either ‘openness’ or ‘secrecy’. Indians are either willing at times to share all personal information or not share it at all. Many Indians are still unaware of how and where their personal data can be used.

Most Indians continue to be oblivious about the dangers of privacy invasion and the several risks it poses, such as discrimination, surveillance, identity theft, cyberbullying, cyber extortion, profiling and behaviour predictions. Awareness about privacy issues only becomes real to people when they are individually affected by a privacy breach or in case of a large-scale event involving data or technological giants.

---

2. Balancing the Secrets of Private Disclosures (Routledge, 1999), Sandra Petronio
Organisations and their roles in privacy protection: Post the implementation of the General Data Protection Regulation (GDPR) for citizens of the European Union (EU) in 2018, there is now a heightened sense of privacy awareness within organisations, with respect to customer data.

But organisations need to understand that privacy is not limited to customer data or the IT department anymore. Data itself has become omnipresent across organisations as data or traces of it can be found in human resource (HR) records, employee behaviour records, data analytics conducted by marketing departments, biometric records captured for attendance, financial records, etc.

In simpler terms, secrecy is maintaining the confidentiality of any information under stringent lock and key measures, whereas privacy is about being responsible with someone else’s data. A common mistake companies make is that they often look at certain aspects of data protection and conclude that since it is a compliance requirement, removing excess data and securing what is left is a good enough measure to ensure data privacy.

The benefits and value of creating business insights from data are gradually expanding and businesses need to re-engineer their privacy strategies as technological innovations such as artificial intelligence (AI), big data and analytics are increasingly being used by organisations worldwide. The true value potential of data can only be unlocked when privacy policies are built contextually, are aligned to an individual’s choice and compliant with laws and regulations.

Privacy is multi-dimensional in nature. It incorporates risk evaluation, interpretation of relevant laws, having in place the right security controls, auditing and monitoring data control sets, and strategising data privacy programmes to design systems that are in line with privacy requirements and regulations. Given the multi-dimensional aspects of privacy, an organisation’s approach towards securing privacy needs to be multi-disciplinary as well.

The author of the article is from PwC and the views expressed are personal.