Significance of Data Privacy in Indian IT Industry

- *A Brief Perspective from Infosys*

Privacy is about giving an individual, choice on what personal information about him or her is collected and shared with whom, and used in what manner. While some of the personal data such as health information, religion, date of birth, address, originates from the data subject, there is another form of data which may be created by an organization or by a public body with whom the individual is associated. Examples of later category of data are : results of performance evaluation of an employee during annual appraisal, credit rating by agencies, web search behavior, criminal prosecution records with Police. Regardless of where it originates, disclosure of such data to unintended recipients and unauthorized processing can cause distress and harm to data subject, apart from financial impact to the organization and regulatory non-compliance.

Privacy as a need in the society existed since centuries, and laws on data privacy mostly started getting enacted in several countries from late 1900s. But it is only with developments in the field of ICT and increasing digital convergence in the last few decades, that introduced much greater opportunities for easy exploitation of personal data by corporates and government, for commercial or other unintended purposes without consent or knowledge of data owner.

Protection of personal data is becoming a priority for the Indian Corporate sector, driven by stricter regulations on data privacy and increasing global business operations. Due to outsourced work, the Indian IT industry in particular has the additional responsibility to protect data of end-consumers from various countries, with exposure to much wider data protection regime. It is therefore imperative that the industry not only assign required focus to data privacy but may also use it as differentiator. While this importance cannot be undermined, privacy is *not an absolute right* and most data privacy regulations allow organizations to a reasonable extent, to balance it along with other conflicting interests such as security, need to comply with other laws or contracts, and business operations to some degree.

This article dwells on some of the key perspectives for IT Industry to consider on data privacy.

Treat Employee Privacy needs, with same importance as for Clients :

When it comes to deploying data privacy initiatives, the privacy of employees in our organizations must also be given equal priority, regardless of external drivers. In India, it is only in the recent times that focus on Privacy is gaining prominence and initiatives such as UIDAI being implemented for the benefit of society, also helped bring to the forefront, the need to strengthen regulations around data privacy. The current Indian regulation to protect sensitive personal data – 'the IT Rules 2011' does not bring any distinction between various data subjects such as employees, customers, when it comes to the requirement of privacy measures that an organization need to deploy. Hence it is important to keep the needs of all stakeholders in view while deploying data privacy controls. It is only when we learn to respect each others' privacy at workplace, at home, among friends, that it will become a culture rather than merely fulfilling a client requirement. Protecting customer privacy will then become more of a habit than a duty.

Play the role of facilitator, more than a control function :

Like any regulatory function, it is tempting from organizational risk perspective to assume a conservative position and thereby cause roadblocks to any innovation & development that has the potential to cause privacy breaches. The pace at which technological developments are taking place, with ever increasing possibilities for seamless flow of data across systems, we may not see corresponding development in laws at the same pace to regulate these developments. Laws are often not intended to be prescriptive to the extent of regulating each technology. The role of a Data Privacy function instead should be to proactively engage and collaborate with solution developers and see how a solution can be engineered right from design stage to minimize scope for privacy vulnerabilities. There is also an important role for corporate legal function in this area, in terms of defining appropriate contractual safeguards, particularly when the solution being developed and deployed pertains to more than one party, for instance in case of a Public Cloud or SAAS.

Participate in Initiatives on Strengthening Data Privacy environment in India :

Active participation is required from all organizations – particularly the outsourcing industry, to deliberate on data privacy cross border issues affecting growth of business. There is significant business not being outsourced to India due to the perception of inadequate data privacy regime and implementation in the Indian industry – more so from European countries perspective. In this regard DSCI and NASSCOM has been closely working with the government over last few years to strengthen the position of the country, and there is significant progress made as we all know. But there is scope for more organizations to come forward and support in this initiative, for the benefit of their own business and for the benefit of our country.

Enterprise-wide involvement in Data Privacy :

Data privacy is a cross-functional responsibility. Personal data is processed in any organization by multiple functions, to name a few – Sales & Marketing, Finance, Human Resources and Operations. The responsibility of the Data privacy office then involves defining requirements, developing processes and systems infrastructure to ensure compliance to various regulations & customer contracts, and deploying the same. The responsibility to implement the control measures rests with employees and sub-contractors and concerned functions in the enterprise. Therefore there is a need to create and maintain awareness amongst employees on their roles & responsibilities in implementing data privacy measures, and the message must be driven that every employee has a role to play in protecting personal data of various stakeholders. It is also important to involve various functional groups across the enterprise on an on-going basis. Changes in processes and practices triggered from business need or regulatory developments, is not uncommon and here the involvement of functional privacy representatives helps in bringing such changes to the notice of the data privacy office for timely impact analysis and necessary corrective actions. Moreover changes in one data processing function often affect the processes in another, and possibility of such interconnected changes going undetected is higher in large organizations operating in multiple geographies with centralized data processing.

Privacy is distinct from Security :

Though interrelated, they are distinct functions addressing different needs on protecting information. Information Security emerged as a key function in the organizations and government bodies much before privacy did, and was driven by the need to prevent data access and confidentiality related violations. The data involved here may pertain to various categories of information such as source code, privacy of customer data, a company's IP, business data, sensitive government data, depending on the industry or the government body. Security has a broad coverage on all types of data & information, and is driven by various needs, one of which is data privacy. Privacy on the other hand, though focusing only on personally identifiable information, has in addition to security, several other dimensions such as providing notice and choice to data subject, ensuring legitimacy of collection & purpose of processing, data quality, providing data subject access. These aspects do not generally form part of a conventional information security management function and may often need a different structure to be effective. Hence while alignment between the two functions is crucial, the two need to have separate focus.

Author: Srinivas Poosarla, Associate VP & Head, Privacy & Data Protection, Infosys Ltd., India