Data Privacy: Transforming Challenge into Golden Opportunity

*Dominic Karunesudas

Data is the new age oil of emerging global businesses. It keeps the business focus at the cutting edge of innovation, research and market development. This further complements to stay ahead of the competitors. Big data analytics, artificial intelligence, machine learning and natural language processing technologies are converging to get deep into the mind of the customer to prejudge and precisely predict her needs and in turn place an irresistible, difficult to resist offer to her way ahead of anyone else. Many enterprises today are selling these insights which have a huge potential of applications as well as gross abuse. It is said that Google, Microsoft and Apple of the day know more about you than your spouse.

Privacy has historical roots in philosophical discussions, the most well-known being Aristotle's distinction between two spheres of life: the public sphere of the polis, associated with political life, and the private sphere, associated with domestic life. More systematic treatises of privacy in the United States did not appear until the 1890s, with the development of privacy law in America. Since the Nazi regime, Privacy in the public domain was a challenge against own government. Knowing too much about its citizen's private life and thereby subjecting them to the control of the government of the day or few powerful persons has been an established and legally recognized threat. Many nations, including the US, explicitly protect citizens from intrusion in their private lives. Though India does not have any such actionable law, the constitutional protection is provided through the Article 21. The Government is subject to the due procedure established by the law. For example, reasonable restrictions are placed on the government from tapping under the Telegraph Act and the Information Technology Act.

However, with the advent of the Internet and the creation of a globalised village, everyone on the Internet is not more than 3 degree away. The tools and applications allow collecting as much data as possible on the user, in the name of better service offerings. The governments across the world has started deploying the similar technologies as the corporates to collect precise data on its respective citizens. Therefore, this rush to get as much personal data on an individual needs to be contained as the possible harm arising out it has become significant. The losses due to breach in Sony Entertainment and Equifax is still unfathomable.

The Indian Supreme Court in Justice KS Puttuswamy vs. Union of India judgement has clearly established that privacy is the Fundamental Right of a persons under Article 21 of the Constitution of India. The Supreme Court has also directed the Union Government to bring legislation on privacy.

First Justice Shah Commission and later Justice Srikrishna Committee submitted their reports on privacy after extensive public interaction came up with draft legislation in 2018. The government worked on the draft given by Srikrishna Committee and finally Privacy Data Protection Bill 2019 (PDPB-19), that was placed in the Parliament on 11 Dec 2019.

The PDPB-19 has been referred to the 30-memeber Joint Parliamentary Committee. It is expected that the bill will be back in the Parliament for enactment in monsoon session or winter session 2020. Therefore the Privacy Data Protection Act likely to be in force by early to mid-2022. This may sound as if there is enough time with the industry and it may be too early to look at this issue. However, the fact is that these months have provided an opportunity for corporate, Government and PSU leaders and directors to complete many pending tasks which would have been difficult to be achieved within 18 months window. In fact it is better to convert this challenge into an opportunity by dealing with it in a structured and planned manner.

Salient feature of Privacy Data Protection Bill -2019

a) The proposed privacy bill may be in front of JPC and may undergo some changes but as on today the salient feature of the proposed personal data protection law are:

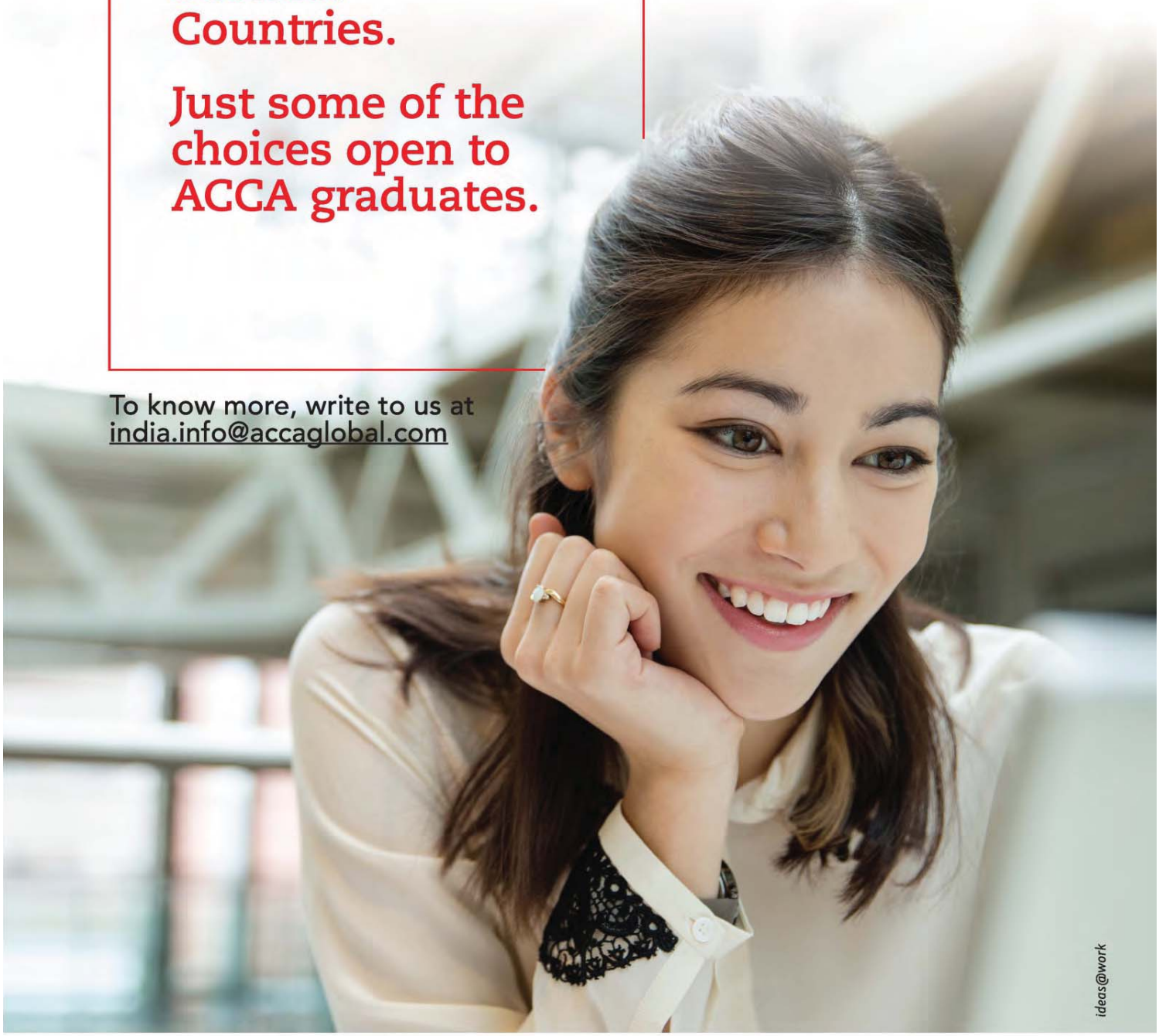
b) It will create a significant risk to an organisation, may be

ACCA Think Ahead

Industries.
Sectors.
Countries.

Just some of the choices open to ACCA graduates.

To know more, write to us at
india.info@accaglobal.com



to its very survival through stiff penalties up to INR 15 Crores (about US$ 2 million) or 4% of worldwide turnover whichever is higher. The Data Protection Authority will have power to stop or suspend any process which may have significant impact on the business. Data dependent companies may require restructuring their business model itself.

c) Privacy is a new concept to Indian organisations as well as society. The change in organisational culture, even understanding few concepts going pose serious challenges.

d) The law places obligations on the organisations who take decision on data processing (called as Data Fiduciaries). These obligations are in terms of limitation of purpose & storage, accountability, prohibition on processing unnecessary personal data. Consent and Notice are primary mode of control of most of the organisations. There are only limited situations where consent is not mandatory, primarily for government related activities, employers and to handle situation like fraud detection, Information Security, mergers & acquisitions etc.

e) The law will empower individuals over their personal data to have oversight on her personal data, correct/update it and in extreme case erase it. Individual called as data principal can also seek her data to transport to other entity for similar purpose through portability rights. The organisations therefore need to be ready for responding to the requests of data principals in a timely manner.

f) Data Fiduciaries will be expected to embed Privacy by Design (PbD) in its all functions – managerial, organisational, and technical and business practices. There will be a certification mechanism based on the privacy by design policy. This policy will not only be on paper but will be subject to audit. The auditors will be empowered to assigned data trust score of a company which will enable users to judge and use the services accordingly. Hence data trust score may be a point of competition.

g) There will be three types of Data Fiduciaries viz simple Data Fiduciaries, Significant Data Fiduciaries (all those who crosses a threshold) and Guardian Data Fiduciaries (who primarily handling data of Children below 18 years old). Some companies may assigned as significant data fiduciary by order and will be subjected to additional compliance requirements.

h) Similarly there will be three types of personal data viz. simple personal data, Sensitive personal data (as will be defined in law and by the Authority) and critical personal data (as will be promulgated by the Central government time-to-time). Organisations handling sensitive personal data will be required to place additional security measures to safe guard it and will not be allowed to process (including storage) it outside India without specific approval of the data principal. Processing outside India of critical personal data will be totally prohibited save some specific circumstances related health, safety or provided for by the government.

i) Organisations will be required to put appropriate security measures in place and undertake privacy risk assessment through Data Privacy Impact Assessment (DPIA).

j) Appointment of Data Protection Officer and Data Protection Auditor is mandatory for all significant data fiduciaries but maintaining proper records as listed is necessary for all data fiduciaries.

k) The bill provides for exemption of the specified government agencies & law enforcement agencies the law from part of full application of the proposed law.

l) The law will not be applicable for processing certain research, archival and statistical purposes also

m) For purpose of innovation the law provides for sandboxing mechanism for initial period maximum of 3 years for the research & product development.

n) To govern the privacy law, new entities – Data Protection Authority of India, Adjudicating Officer (under the Authority) and Appellate Tribunal (independent of the Authority) will be created.

o) Code of practices will be put into place while the authority will have powers to order for inquiry, sought information, documents, search & seizure, and audit.

p) Re-identifying hidden (de-identified) personal data can lead to jail term up to 3years or fine and such offences will be cognizable and non-bail able.

q) When offence or breach of law is committed by a company or the State then along with the company or the State, the persons responsible for the company, head of department and actual offenders will proceeded against according to the statute.

Due Preparation time

Compliance with new privacy regime will be like rebooting the whole business for some of the companies, but for most it will have significant impact. An approximate time required by a significant data fiduciary is listed below to estimate time and budget required by the company or department. It may be noted that the delay in enactment of the PDP Bill 2019 provides the necessary cushion and allow more structured approach to make necessary changes.

- It is expected that after the key member of top management become aware of the business impact of PDPB it will take considerable time to bring majority of

Reach Landmarks of Chennai through

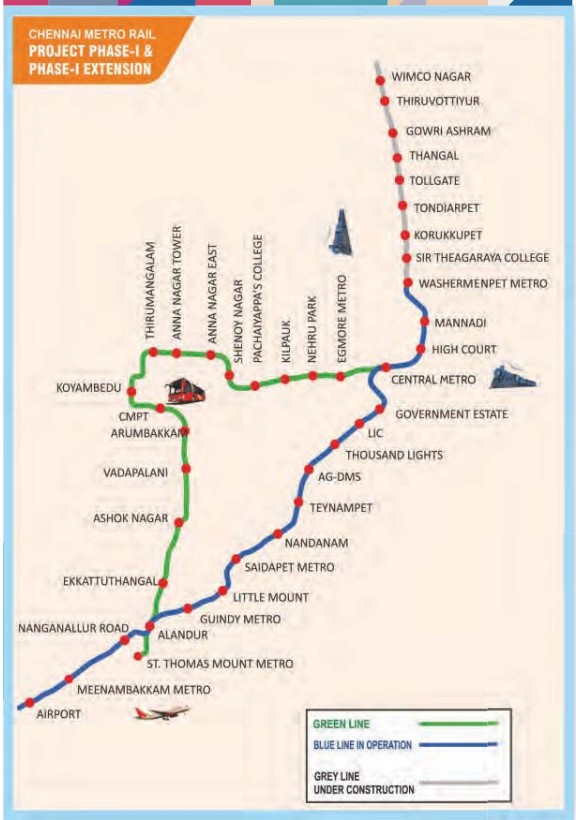
CHENNAI METRO RAIL

CHENNAI METR RAIL C NNECTS AIRP RT – CMBT-EGM RE-CHENNAI CENTRAL – HIGH C URT – GUINDY INDUSTRIAL ESTATE – EKKATUTHANGAL IT PARK AND MAJ R C MMERCIAL DESTINATI NS

- 6.7• crore passengers have travelle•in Chenna• Metro R•il from 29th June 2•15 to 29th Feb 2•2•
- More than a lakh passengers travel in the Chenna• Metro R•il everyday

Facilities and Services in Metro Stations and Trains

- First Class Secti•n and W•man •nly C•ach with L•wer Hand Grip
- Travelat•r Facility fr•m Chennai D•mestic and Internati•nal Terminals t• reach Airp•rt Metr• Rail Stati•n.
- Smart Cards are available at all Metr• Rail stati•ns f•r Seamless Travel.
- Easy Access t• all Star H•tels and c•nsulates fr•m Chennai Metr• Rail Stati•ns.



ng ing Chennai Metr Rail Pr jects

Extensi•n •f the Phase - I fr•m Washermenpet t• Thiruv•ttiyur/Wimc• Nagar c•vering 9. 51 km expected t• be c•mpleted in 2 2 .

10% Discount on Travel Card

50% Discounted Fare on all Sundays & Government Holidays.

CHENNAI CENTRAL (SCC) TO AIRPORT (SAP)	CENTRAL	AIRPORT
First Train	04.32 Hrs	04.37 Hrs
Last Train	23.07 Hrs	22.59 Hrs

WASHERMENPET (SWA) TO AIRPORT (SAP)	WASHERMENPET	AIRPORT
First Train	04.23 Hrs	04.22 Hrs
Last Train	23.00 Hrs	23.01 Hrs

the top management on board (likely time 3-6 months).

- Designing strategic roadmap is possible only after a clear understanding of the impact of PDPB on the business is drawn. And without such roadmap none of the following actions is possible. (about 3 months)
- Implementing PDPB will consume resources and funds, therefore require structured budgeting. Now is the right time to block funds for PDPB even if fund outflow starts later.
- Appointing Personal Data Protection Management team with competent staff/ Data Protection Officer & auditors. (One month).
- Several iterations of Privacy Data Impact / Risk Assessment will be required which itself can take 12-18 months.
- On IT technical side it can take anything 6-18 months to implement changes at network, databases, application and websites. This includes listing out and segregation all personal data and their need for business can be complex and strategic decision making may consume as much as 9-12 months.
- On Security implementation to ensure privacy, it likely to take 9-15 Months in case starting from scratch and security maturity level 1.
- There will need to change Organisation Culture. In the Indian environment where concepts of privacy are weak, it can be a tedious task and may require several rounds of culture change intervention from the management. It may take several years for an effective privacy culture in an organisation.
- Redrafting contracts and managing relations especially imposing liabilities for non-compliance and closing it expected to take 3- 12 months.
- Encryption policy, destruction policy and responding to Data principle requests are intertwined with several other factors - technical, managerial as well as legal. This can take as long as 12 months to implement.
- Many of these issues are interlinked and sometimes sequential hence actual time to implement will extend way beyond 24 months.

Closer to the date of compliance the charges by the competent consultants will shoot up. There will many incompetent, fakes or fly-by-night-operators also set up shop. Hurriedly undertaken such complex task can leave gaps impacting proper compliance. Hence, it is prudent to start early and do a thorough job. The first step thus is to understand the subject from a business perspective, and not only from legal or technology perspective

Seizing the Challenge

The Compliance with the proposed Personal Data Protection Act may sound challenging and it is indeed complex and challenging. However this challenge can be converted into opportunity by early adoption. Of course, there are many things required to happen before there is full clarity. First the JPC may change the bill, then rules and regulation will define the final implementation contours and code of practices will impact at nuts & bolts level. However a good adviser can decipher as to which provisions of bill will be retained in the Act with no or minimal changes. For example there may not be major changes in rights of Data Principle. The process of consent may not be different from the present Bill.

The technical risk assessment maybe embedded as a part of process. ISO/IEC 27001 and 27701 can be implemented right away. An effective implementation of these standards can take 6-18 months. New secure approach will be required in post COVID-19 environment where large number of employees may work from home.

Any company who gets early Privacy-by- Design policy certificate and good Trust-Score will be ahead of competitors and late starters may in fact have to close shop. Therefore an early start and reorientation of the organisation with its leaders and the board members leading from the front can convent this challenge into opportunity

***Mr. Dominic Karunesudas** is a prominent cyber security and technology entrepreneur with over 19 years of professional experience in high technology consulting, advisory and product development such as in cyber security/data privacy, blockchain, AI/ML, drones, along with e-governance, digital media and technology policy. He is Director at Technitics Consulting Pvt Ltd., and former editor of technology with the Times of India Group, CNBC TV18 and Web18, Indian Express group. He also briefs the PMO, national security agencies, the armed forces of India and the private sector leaders on matters related to applied technology and cyber security for national and economic security.*