Data Protection Journal of India

No: 3/2021: 30th July **2021**

THE VALUE OF DATA

Journal published For

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

Publisher: Na.Vijayashankar

What is Inside

From the Chairman's Desk

THE VALUE OF DATA

The last few months in India in the Data Industry has seen many important developments. On the one hand we had the controversy of Twitter claiming itself to be the "Champion of Freedom of speech" while the Government accused them of a motivated campaign to malign the country's image as a democratic society. WhatsApp deferred enforcement of its new Privacy Policy in India. Twitter and WhatsApp challenged the sovereign powers of the State in the belief that there is a global pressure on the country to refrain from taking any coercive action against these tech giants. Many Courts have admitted petitions against the implementation of the Intermediary Guidelines and Digital Media Ethics Code which was introduced from February 25, 2021.

Amidst these developments Zomato made a successful IPO and created a market capitalization of over Rs 1 lakh crores though it is still a loss making company. Through this issue, the traditional concept of "Institutions" and "High Networth Investors" funding the pre-profit making activities of a Start up and stock market investors funding the post-profit making activities appears to have been given a go by. Just as other "Derivatives", the "Equity Shares" per-se have become "Derivatives" on which investors can place their bets irrespective of the profitability.

PDPSI (Personal Data Protection Standard of India) had introduced the concept that "Value of Data should be made visible in the Balance sheet of an organization" as part of its implementation specification. This issue of DPJI discuses in depth how "Data" may be valued and whether it can be brought into the financial statements and whether there is an acceptable method by which the value representation can be acceptable to the accounting fraternity.

The Zomato issue has also opened up the thoughts that part of this corporate valuation may depend on how data is used by the companies and whether the forthcoming data protection law in India would have any impact on the profitability of these companies.

Along with this valuation aspect, there is a felt need for the industry to consider how the value of data can be transferred to legal heirs on the death of an individual and whether there should be a legal basis for the inheritance of the data value. An internal committee of FDPPI members deliberated on this aspect and has come out with a preliminary report which is part of this issue.

We hope that the thought of "Valuation of Data" and "Transmission of Deceased Data Assets to the legal heirs" as discussed here would be useful to the community.

During the quarter, FDPPI is proud to have completed its first engagement with DNV by conducting a training for "PDP-CMS" auditors which was successfully concluded in July 2021. Over 20 senior industry professionals successfully went through the program. During the quarter, FDPPI also launched the "Privacy and Youth" program to start student chapters in colleges. I congratulate all the members who contributed to the success of these projects.

Naavi

News Section

FROM THE NEWS ROOM

1. Bureau of Indian Standards released a new standard document under the number IS 17428 as the Data Privacy Assurance requirements and Guidelines. This framework tries to address the requirements of personal data protection by Indian organizations on the lines of ISO 27701.
2. Indian Courts started enforcing the "Right to Forget" before the PDPB2019 becomes a law. Delhi High Court upheld the right of an accused who had been acquitted in a narcotics case to place a restriction on search engines picking up and displaying the judgement where the name of the accused got mentioned. Orissa High Court in an earlier decision had also upheld the right to forget with a detailed discussion on different aspects of PDPB2019.
3. Twitter launched a protest against the new Intermediary guidelines by challenging the regulations as inhibiting free open public conversation. Twitter refused to appoint Compliance officer as required by the guidelines and took the issue to the Delhi High Court along with WhatsApp. A war of words ensues between the MeitY and Twitter on the promotion of "Toolkit" on twitter, for destabilizing India.
4. Domino's-Jubilant Food works suffered a major data breach in which 18 crore data sets were compromised and sold on the Darkweb. The sale value was about Rs 5 crores per buyer. However, the share price of Jubilant did not have any adverse impact and from around Rs 2729 on April 12th, it is today at Rs 3651 indicating that the share price is not sensitive to data breach incidents.
5. Air India also suffered a data breach of 45 lakh data sets containing sensitive personal data. The value of the data breached could be estimated at around Rs 31500 crores and could be a revelation to the Company in its negotiation for its offer of sale.
6. EDPB announced the final version of its recommendations on the supplementary measures to be followed in cross border data transfer following the Schrems II decision, correcting some of the aberrations in its earlier order.
7. Ollie Robinson a Test cricketer from England was suspended following a revelation of an old set of tweets which brought to discussion the "Right to Forget" and the need to place an "Expiry" date for tweets.
8. Zomato made a successful IPO placement at a premium of 7500% despite the company yet to start making profits.
9. A report by Amnesty International indicating discovery of a list of potential 50000 targets for use of Pegasus by an Israeli company NSO, including 300 Indians raised a debate in the Indian Parliament about the possible use of the Spyware against journalists and political opponents in India. In a unique move a Judicial commission was instituted by a State Government to probe the matter.
10. TransUnion, (the partner for TransUnion Cibil) faced a potential damage suit in the Supreme Court of US due to a false positive generated in an identity check where an innocent person was flagged as "Being in the Government watch list of terrorists", raising the importance of "Quality of data".
11. The presentation of the PDPB2019 in the Parliament was extended to the next session.
12. Rajeev Chandrashekar, a well known IT entrepreneur took over as Minister of State in the Ministry of Information Technology while another Technology expert Mr Ashwini Vaishnav assumed office as the Minister of Telecommunications and IT.

(For more detailed discussion on the above news bits, please visit www.naavi.org and www.fdppi.in)

Knowledge Section

DATA DRIVEN ORGANIZATIONS

"Data is Oil" is a familiar phrase that represent the aspiration of the industry on how Data may be capable of defining a new corporate order in the world. Just as discovery of Oil fields in the Gulf changed the economic face of earth, "Discovery of the economic potential of Data" will change the economic face of the business environment. If the loss making Zomato gains a market capitalization of over Rs 1 lakh crores without corresponding tangible assets in its possession, If Bitcoin can command a value of USD 40,000 without any backing of law or an asset, there is no doubt that "Data" as an "Asset" needs a very serious look from all the Corporate managers.

Apart from the "Derivation of an enterprise value" from out of the "Data Assets" owned by an organization, an organization looks at using Data for improving its productivity and pursues the path of "Digital Transformation". A "Data Driven Organization" is therefore such an organization where "Data" drives better value to the enterprise by increasing its efficiency of current operation.

A "Data Driven Organization" (DDO) has to identify how Data can improve its decision making capacity and proceed to acquire such data. Some of this data may be generated from within an organization and some may be acquired from outside.

The "market information" of who is our customer, why does he buy what he buys?, What price he is willing to pay?, how are my competitors doing?, how is the environment changing?, are any new regulations coming up that affect my business? etc.. are all "Data" that can be gathered from outside and help an organization to frame its business policies.

Internally, data on how our employees are motivated, how our production system is working, how our finances are shaping up, how much of cash I am buring out?, how our creditors are building up? How our debtors are repaying? etc., are gathered as :Internal Data" by the organization.

In the Industry 4.0 scenario, data is part of the manufacturing process as the behaviour of machines is automatically calibrated with the data generated during the process of manufacture itself or a real time basis.

In many situations, "Data" is the raw material of production and transforms itself to a more valuable form like a raw material or a semi finished getting converted into a finished good and is sold for value. The special character of "Finished Data Product" is that it is "Replicable" and

unlimited instances of the finished product can be created with one original instance of a finished data product. In such situations the cost of producing one finished product is distributed over infinite saleable instances and the number of units that can be sold depends only on the demand. The cost of production has to therefore be considered as cost of creating a "Fixed Asset" that can roll out finished products on demand.
In the manufacturing sector we also have a situation where "Data" does not limit itself to creating other value added finished data products but converts other physical material into a physical finished product through 3D printing.

We therefore can divide DDOs into different categories based on how the Data is used

1. DDO where Data is used for better decision making by business managers. This includes all companies where data is available for the business executives to take appropriate business decisions including which market to enter, what products to produce, how much to produce, how much to charge etc (Decision makers)
2. DDO where Data is used to drive the machines through automated dynamic process corrections and process decisions. This includes all the manufacturing processes which use Computer controlled process and can take dynamic production decisions such as resetting machining parameters. It also includes such activities such as robotic surgery. (robotic production units)
3. DDO where Data is the finished product in data form. This includes the typical software companies, AI and ML developers, Data Analytics and Big Data Companies. It may also include content aggregators, entertainment companies, OTT platforms, Gaming companies, Education companies etc. It also includes companies which provide services and in the process gather information which is converted for its own benefit in some form, such as the Googles and Face Book or Amazons and Zomato. We may also include the "Crypto Companies" who develop "Binary Documents" and create a value around it by building a "Perception" for which customers may pay value.(Data Innovators0
4. DDO where Data creates finished product in physical form. The 3D printing companies which produce finished goods through the conversion of a raw material base into a finished product through 3D printing technology. (3D printers)

The requirements of each of these categories of DDOs in terms of types of data required, quantity and quality of data required in raw or finished or semi finished form, the need for accuracy, reliability, timeliness etc will be different.

Accordingly the value perceptions about data will also vary according to the type of DDOs. The concept of "Data is in the beholder's eyes" as per the "Theory of Data" applies in determining the value of data since the unitality of data in different data driven organization is different.

For an organization to be a successful data driven organization

a) It has to create a "Collection of Relevant Data". This may require collection of data in the first place and to filter it as may be required. The data scientists have to device methods of cleaning the data and prepare the data for further consumption.
b) Data should be accessible by the stake holders in a timely and reliable manner. For this purpose the quality of data and its availability has to be preserved as per the principles of Cyber Security of "Data Integrity" and "Data Availability". Protecting data from authorised access is part of managing the risk of loss of reliability and hence Cyber security principles of Confidentiality, Integrity and Availability are part of the requirements of a Data Driven Organization
c) Collection and use of Data has to be in accordance with the laws applicable. In case the data collected is personal data, there will be need for compliance with the relevant data protection laws and hence a data driven organization has to focus on compliance of personal data protection laws.
d) Data should be queryable in the sense that data users should be able to easily configure their own business related queries and generate useful responses from the data analytics.
e) For an effective use of Data Driven decision making, the system should be capable of sensing corruption of data and the possible misleading decisions that may follow. Hence self correction intelligence and flagging of potential threats to usability of information need to be built into the data usage mechanism since the dependency of decisions on data will be high in such Data driven organizations.
f) Ability to switch off the automated functions and prevent continued malfunctioning if any which could be considered as industrial accidents, is part of the security that needs to be built into the systems of a DDO.

Depending on the maturity of an organization in using Data for its activities, organizations may be classified as "Transformational", Experienced" and "Matured".

A transformational DDO may use data analytics for prescribing actions to drive most of its decisions, while the experienced DDOs may use it for tactical decision making for the organization while the Matured Companies may go a step further in using Data for developing long term strategy.

"Being a Data Driven Organization" is the new Corporate objective in pursuance of greater efficiency and in the process "Data" acquires "Value" in different dimensions. One of such dimension is the "Monetary Value of Data" which is sought to be unleashed through the "Non Personal Data Governance Law" which is being planned in India. The personal data protection law which is currently available in the form of ITA 2000 and likely to be fortified with the Personal Data Protection Act will also create a value perception for "Personal Data" though the monetization of personal data may be restricted with the "Consent" mechanism like the Intellectual Property value realization.

The "Digital Transformation", "Building a Data Driven Organization", "Discovering the financial value of Data" are therefore going to be interesting professional pursuits in the days to come.

ENTERPRISE VALUE

A Value of an enterprise is computed from with several objectives. Investors look at the value of an enterprise per equity share as a valuation of their investments.

Essentially two methods are used for this purpose namely the Market Capitalization of shares which is to multiply the stock market price by the number of shares or the Value computed out of the Book value of the shares based on the accumulated networth of the company.

Market capitalization is based on the investor sentiments while the Book value method is based on the accounting standards. Investors also use Price to Book value per Price to Earning per share as yardsticks to check if the current market value of the shares on the stock markets is aligned to the earning capacity of the company.

In the current situation where investment sentiments are driven by the "Perception" of investors created through the publicity around a company or its shares, there is no strict correlation between the Price to Earning ratio and the stock market price.

The investors look at the share only as a reference instrument and trades the shares on the basis of sentiments. This is a "Derivative Mentality" similar to the valuation of "Crypto Coins" which may not have any basis for valuation but are still bought and sold vigorously.

Most shares like Zomato are in the class of "Crypto Shares" where underlying profit is of no consequence and the Book value or Price to Earning ratio are not considered elements of valuation of the shares. Hence market capitalization as a measure of "Enterprise Value" is sentiment driven and cannot be considered as a reliable basis for organizations who may like to lend money to an organization.

On the other hand, the traditional method of valuation of an enterprise is as an aggregation of all its assets at a value which is based logically on the value that can be realised if the enterprise is sold as a going concern.

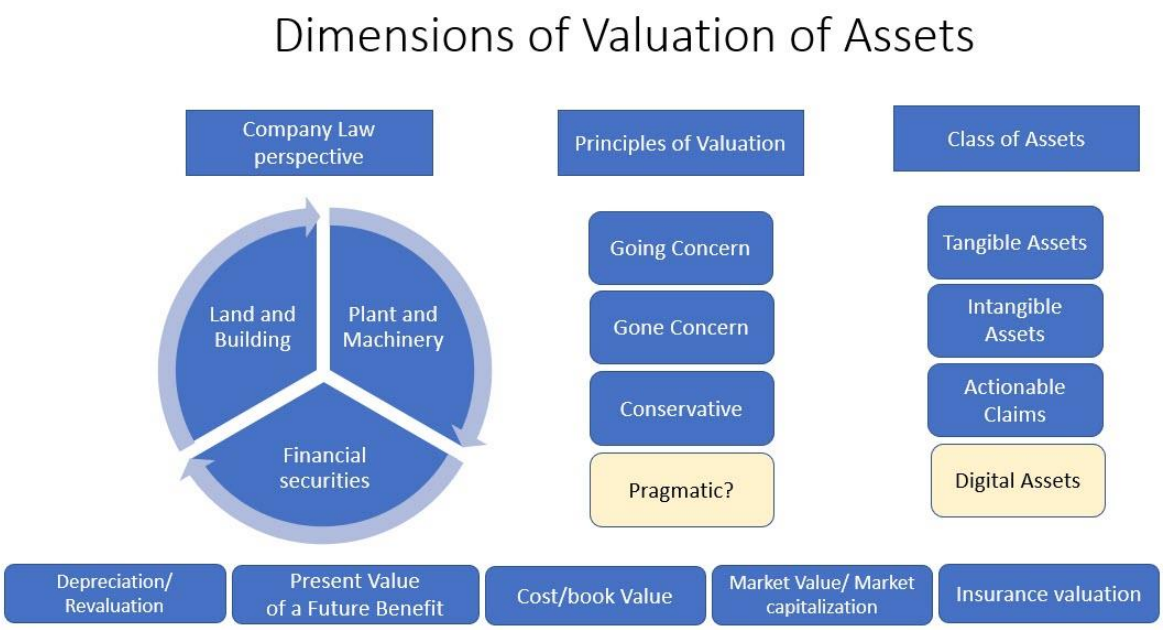
As a going concern, an enterprise looks at its assets such as Land, Building and Machinery as assets which are expected to provide benefit to the company in the long run by rolling out end products. Such assets are tangible assets which have a physical existence and can be sold or leased or otherwise transferred for a value which the accountants try to capture as realistically as possible in the financial statements.

Certain assets are classified as "Current Assets" when they are likely to be converted or meant to be converted into cash within one accounting period.

Assets which donot have a physical existence are classified as Intangible Assets which includes the valuation of Goodwill, Trademark, Copyright or Patent Right.

Money receivable under contractual arrangement maybe classified as “Debtors” if they are business related.

There are certain dues which are at the discretion of the company or on the occurrence of a contingent event such as Insurance Claims. They are treated as “Actionable Claims” and based on the case to case assessment, the accountants may classify them as “Contingent” assets or “Miscellaneous Assets” or “Deferred Receivables”. Conservative accounting principles avoid accounting of “Contingent Assets” as an above the line item and either provide information about such assets as “Notes” below the line or as “Contra item” where they are added as both an asset and a liability.



The intangible assets such as Goodwill which are self calculated and not “Bought for cash” are not considered for the valuation of profit of the company and its value gets reflected as “Special Reserves” not available for distribution.

Certain assets like land are often “Revalued” and the surplus created in the process is also credited to a “Revaluation Reserve” not available for distribution.

When businesses are acquired or mergers effected, the value of intangible assets may get converted into real assets in the books of the buyer since he has paid cash to acquire it. But they still are considered different and may be excluded for many financial ratio analysis in lending decisions.

It must be recognized that land and building may be fixed assets in companies where they are bought and used for the business for setting up a factory or office. But in a real estate company, land and building may be considered as “Current Assets”.

These principles of valuation of assets are well established in accounting and in this scheme of things “Data” has not been considered as an “Asset” which can be brought into the balance sheet.

While we look at “Data as oil” or observe that Google (Rank 73), or Amazon (Rank 2) or FaceBook (Rank 34) have become fortune 500 companies solely on the basis of their data

assets, one wonders if their data assets are visible on the balance sheets since their rankings may be based on annual revenues.

If we look at the stock market sentiments where "Derivatives" are traded and market capitalization is created through sentiments, accountants wonder if the world view on the use of financial statements for assessing the worth of a company has any meaning in the days to come.

The statutory audits of companies are today focussed on presenting a true and fair value of the assets of a company in the balance sheet. But investors seem to ignore the value of the assets or the P&L account which renders the system of statutory audit of financial accounts meaningless from the point of view of investors.

On the other hand, "Data Auditors" are emerging as a new class of "Auditors" who look at "Data" as an asset and going forward, we may not be surprised if investors would be looking at the "Data Audit" more closely than the "Financial Audit".

Recently, in India there were two major events where the valuation of Data assets of the company came for discussion.

Firstly, Net4India, which was one of the first companies in India which started business as "Registrar of Domain Names" and had more than 3 lakh customers who were committed to renewing their domain name registrations and hosting with the company and constituted a "Data Asset" for the company worth more than Rs 100 crores, was declared insolvent since the valuers did not take into consideration any value attached to this customer list. The NCLT took the land and building owned by the company and perhaps the computers and network equipments but ignored the value of the customers who provided an assured stream of income to the company.

With such a logic, even if Net4India had owned the spectrum rights for Telecom services, it would have gone unvalued since it is a "Data Asset" or "An asset which is a pipeline for converting data assets into cash as part of a telecom business".

The second incident was that TransUnion which is a NYSE traded company silently acquired 92% of the shares of CIBIL whose main asset is "Sensitive personal data" of 1000 million Indians and their financial profile. The acquisition was from several Indian Banks in which public had a share holding and there was no discussion on whether a fair value was paid or not. According to the Darkweb value estimates, the value of data owned by CIBIL is worth around Rs 7 lakh crores. But Indian banks who transferred these shares could have transferred it at face value while they are begging before the Government for bailing themselves out of NPA crunch.

In comparison to these two incidents, it is reported that United Airlines and American Airlines in USA were able to raise secured multi-billion dollar loans by collaterizing their "Milege Plus" and "AAdvantage customer loyalty programs", similar to our Air India's "Frequent flyer program". The third party appraisals of the data of these two airline companies indicated that their enterprise value was two to there times higher than their "Market capitalization".

For example United's customer data was valued at $20 billion against its market cap of $9 million and Americal Airline data was valued at $20 to 30 billion against the market capitalization of $ 8 billion.

Further, in the Bankruptcy proceedings of Caeser's Entertainment, Forbes reported that the most valuable of the individual assets fought over by creditors was the data collected over the last 17 years through the company's Total Rewards loyalty program, which gained Caesar's a reputation as a pioneer in Big Data-driven marketing and customer service. Total Rewards is estimated to be worth over $1 billion.

The above incidents indicate that "Not bringing the value of data into financial statements" is a mistake that accounting fraternity of the day are making. In the coming days if a "Data Auditor" provides a report that a company X has data roughly valued at Rs ……. and the information becomes part of the foot note in a balance sheet then the investors who have valued Zomato at 1 lakh crores in terms of market capitalization will flock to acquire the Company X shares and jack up its market capitalization.

Under the Indian Data Protection Act as proposed in PDPB 2019, a mandatory data audit is proposed for all significant data fiduciaries. This data audit is an evaluation of the organization on how the company is complying with the provisions of the personal data protection regulations. The view of the auditor will be provided in the form of a Data Trust Score.

At present, FDPPI is the only organization which is using a framework called "PDPSI" or Personal Data Protection Standard of India to conduct an audit of Personal Data Protection Compliance Management System (PDP-CMS) and arrive at a Data Trust Score. It is interesting to note that the PDPSI framework does have an implementation specification that expects the Significant data fiduciary to provide "Visibility" to its personal data assets by bringing it to the balance sheet.

If PDPSI auditors come up with their assessments and find that a company has valued its data assets at a value N and Confirms the valuation system with its own appraisal, then such a company will have a "Data Auditor's certification of the data value" of the organization which could cause disruption to the stock market valuation of the shares.

It would be interesting to see how this field of Valuation of data develops in India, what methodology would be used, how the valuation would be adjusted for sensitivity or criticality of personal data, quality and age of personal data etc. It would also be interesting to observe how the Non Personal Data would be valued by a "Data Business" as envisaged by the Kris Gopalakrishna Committee on Non Personal Data Governance.

Probably when loss making start ups want to raise money from the public through IPOs, like Zomato or Paytm, SEBI may need to insist that apart from the financial audit, a "Data Audit" should also be made mandatory.

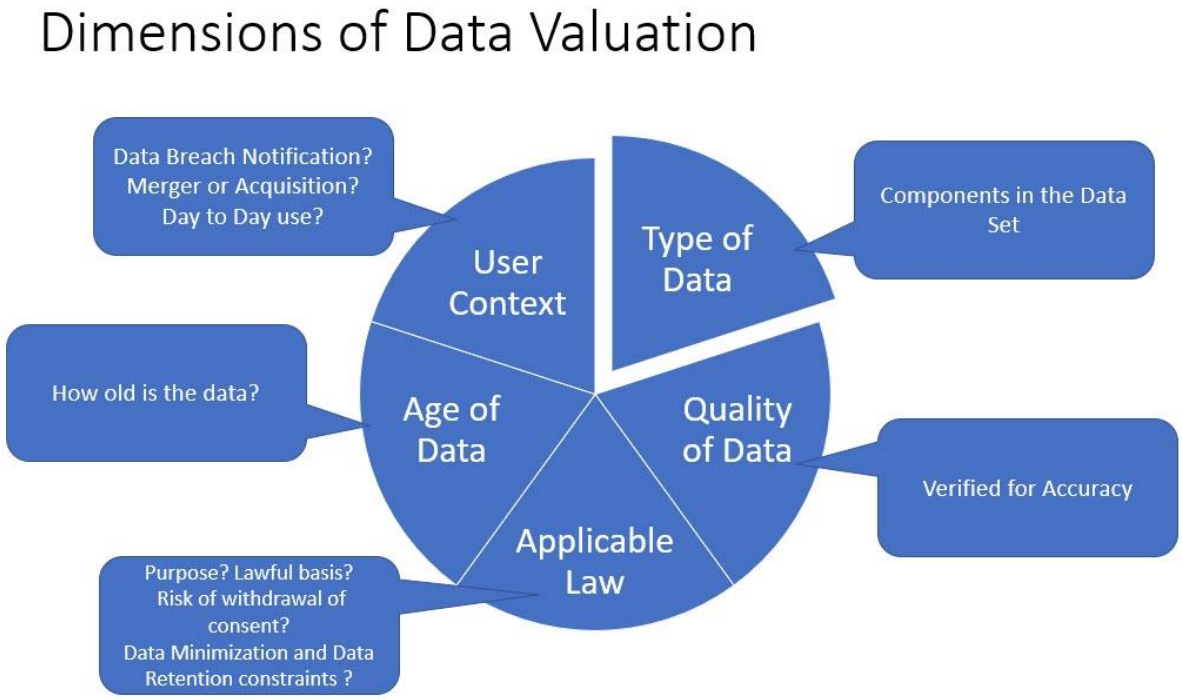
The future of enterprise valuation on the basis of the valuation of underlying assets including "Data" would be a challenge to the accounting community. But this is an area which is very important from the perspective of investor information which is essential for the development of a less speculative secondary market and ensuring that Primary market remains non-speculative to the extent possible.

VALUATION METHODOLOGY FOR DATA ASSETS

When we look at "Data" as an asset and try to assign a value tag, we need to first determine if it can be considered as one of the currently known asset types for financial statement.

Firstly, Data is an intangible asset and therefore cannot be considered as a tangible Fixed asset or a Current asset. Currently the known intangible assets are assets like the good will or IPR which arise out of a valuation. There is an accepted method for valuation of these assets also .

For example the existence of any IPR or even Goodwill is expected to enhance the business prospects of a company. Hence we can calculate the Net present Value of future revenue over a reasonable period representing the life time of the asset with and without the presence of the intangible asset to arrive at the value attributable to the intangible asset.



Cost of acquisition is always a reliable indicator of the cost on a conservative basis. Cost of data can be computed by calculating the direct expenses related to the collection of data in a given period of say one accounting period. Here the cost of people, cost of computers, software etc can be computed for a given period and divided over the number of data sets created to arrive at the unit value of data or even the total aggregated value of all data created. This computation would be relevant only in respect of costs associated with the data acquired for business and used for business decision making. Cost incurred for Data unrelated to business can be excluded.

Market Price of an asset is also an established form of valuation and if available, can be used for Data also. Market value perception may be available through Darkweb or through Ransom ware demands or through specific data breach surveys which are a reasonably acceptable methods to arrive at the value of data in the hands of an organization. Data which is secure may be considered more valuable than data which is stolen and placed in the dark web. Hence a

"Premium" may be attached to the data which is secure in the hands of an organization as a "Security Premium". This may be removed in the event of a data breach.

When a data breach occurs, the security of data can be restored by replacing the breached data with renewed data where possible (eg: passwords which can be reset) and also by covering the misuse of the breached data with an insurance cover (like identity theft insurance) to render the potential of misuse in-effective.

As regards the utility of data which is breached, there may not be much of a difference in value to the organization. But if there are liabilities arising out of the data breach, then they may have to be factored for lowering the aggregate value of the data with the company.

After ascertaining the value of data by different means such as the cost, market value, an expert valuation with averaging of value obtained by different methods can be computed.

The emerging value could be considered as the "Intrinsic value of data" on a going concern basis. Instead of the "Average", some data valuers may take the conservative approach of "Cost" or "Market Value" whichever is less which also would bean acceptable method of arriving at the intrinsic value of data.

This intrinsic value computation may be sufficient to bring "Visibility" of data in the financial statements either as a foot note or as a "Contra item" where the same value is added both for assets and liabilities so that the total enterprise value does not get altered in the books of account.

However, it should be the endeavour of every organization to bring to its financial statement a more realistic and fair assessment of the value of the data asset as a separate "Data Class". For this purpose, it may be necessary for the data auditor to go a step further to assign weightages to different categories of data based on a classification.

For example, if we classify "Non Personal Data" into say Financial data, Market Data, HR Data, Business data, then different weightages may be assigned to these data. Normally organizations classify data as "Confidential", "Secret", "Internal" or "Public". Such classification may require some modification from the perspective of data valuation. A Confidential data may not always be the more valuable in the valuation perspective since it may not be used for generating income. Only when a data has some use, it acquires value. Data which is kept under lock and key is like money hoarded by a miser and may not have real value. In some cases like the "Demonetization" effect, hoarded data may suddenly become useless.

Similarly, when it comes to valuation of "Personal Data", the "Type" of data as "Sensitive" and "What type of sensitive" , whether it is verified or confirmed by the data subject, whether the consent for use is broad etc., could be criteria for assessing the value.

It is therefore necessary to develop a matrix to assign weightage to the intrinsic value (Cost or Market Value) based on different parameters of quality, age, the depth of data set etc.

At first glance, it appears that valuation of data is complicated and it requires an in depth knowledge of the nature of data, the life cycle of data, the laws related to data etc.

There is no doubt that for valuing any asset, an indepth knowledge of the domain would be beneficial and perhaps necessary. But if one analyses the general approach of any asset valuation, the valuer has to display an in-depth knowledge of the industry to which the asset

belongs and adjust several parameters that an inexperienced person may not be able to identify and factor in.

If we take the example of a valuation of a building, we have the land value, value of the construction, whether vacant possession is available, whether there are any litigations potential or real, whether any Government regulations affect the use of the asset etc. This may require the knowledge of Civil construction, the real estate market, law related to property etc.

Similarly if one looks at a valuation of a gem stone, the type of gem, its rarity, the weight and purity etc may all have to be judged and there may not be a standard method by which it can be ascertained without an in-depth expertise.

It is therefore nothing special that valuation of data also requires a certain kind of special expertise. It is possible that the civil property valuers of today or even the Gem valuers may not know how to value Data. But "Data Valuers" may be developed with relevant knowledge so that they will be able to do valuation which is reasonably acceptable to a large section. Just as two valuers may come up with different valuations for the same piece of gemstone, it is possible that two data valuers may also differ in their value perception for the same data. This is also quite natural and should not be considered as a reason not to attempt data valuation and bringing them to the books of account.

In the initial days, the value of data may be included in the financial statements but the financial analysts who calculate the Debt-Coverage Ratio or Current Ratio or Quick Ratio, the Profitability on asset ratio etc may leave out the value of the data asset and continue to use their legacy systems of financial statement analysis. In due course when the confidence of the community on the valuation systems increase, we may be able to develop separate ratio analysis for examining the productive use of data as an asset.

The Data protection and the Cyber Security Community which today have reasonably good understanding of the nature of data need to join hands with the community of valuers such as the RERA Valuers, the Insolvency and Bankruptcy resolution professionals, the Chartered Accountants CA, Company Secretary and Cost accountant Community and arrive at an acceptable method of valuing data both the personal and the non personal variety.

Perhaps there is a need for an inter disciplinary committee to be formed amongst different professional bodies to work towards establishing a "Data Valuation Standard of India". FDPPI may take the lead in making this possible.

HANDLING OF DATA OF DECEASED ASSETS

The data protection laws normally apply to the protection of personal data of "Living" "Natural Persons" because the basic objective of such laws is to protect the Right to Privacy of the Citizen of a country and such right exists as long as Citizen is alive and the Government has an obligation to protect his privacy. GDPR has clearly stated that it is not applicable for deceased persons. Indian law has not specifically stated that the law is applicable for only living persons but it can be implied from the circumstances.

It is however a problem when a data subject leaves his valuable personal data in the custody of a service provider such as Dropbox or Face Book or Google or Twitter. Since personal data is not clearly identified as property, the inheritance rights of such data could be vague. Though Face Book allows limited access to the data of a deceased person, it appropriates the data for its own use. Most other service providers also do the same. Drop box has a clear claim process. Twitter also may have a system of processing the transfer of account to the legal heir though twitter does not contain confidential data in storage like DropBox.

In services where a copyrighted material of the deceased is present or confidential data such as passwords disclosure of which may give access to Bank accounts of the deceased to the receiver are issues that could create problems. It is also possible that some of digital accounts may contain "Crypto Wallet Access information" which could be valuable financial asset on which the legal heirs should have a claim.

Further, the data protection laws often require "Renewal of Consent" and if a data subject does not renew the consent, then the personal data cannot be used further by the service provider.

Keeping these issues in mind and recognizing that in India, a Will cannot be created through an electronic document but the law does not prevent a will to transfer the digital property through a written will, it is essential for Data Fiduciaries to incorporate a policy for dealing with the personal data after the death of the data subject and establish a proper claim process which will stand the test of law.

At present there is no law in India which can create a "Nomination" of a digital asset and hence the transfer of data after death of the data principal cannot be easily resolved by the data fiduciary.

Further if "Data" is an asset and it remains unclaimed, it is the sovereign right of the Government to appropriate the data and the private sector service provider many of whom are foreign companies have no right to appropriate the data.

In order to handle these issues, the PDPSI framework suggests that a suitable policy is instituted by data fiduciaries to handle personal data upon death of the data subject starting from recognizing that a data subject is no longer alive to identifying the legal claimants and transferring the custody through an appropriate manner. A Copy of the suggested policy for data fiduciaries is enclosed below.

Ujvala Consultants Private Limited
#37, Ujvala, 20th Main
BSK First Stage, Bangalore 560050
Web: www.ujvala.com:E mail: naavi@naavi.org: Mob: 9343554943

Draft Code of Practice
And
Draft Policy for handling Personal data of Deceased Data Principals

Objective

The objective of this Policy is to establish a method for handling the personal data of an individual who is known to be or is suspected to be deceased.

Background:

An organization would be in possession of personal data of an individual collected with appropriate informed consent.

The Consent is a "Contract" with an offer document in the form of a Privacy Notice" by the Data fiduciary and an acceptance by the Data Principal through an affirmative opt-in. In certain cases, the offer is in the nature of "Invitation to offer" which is accepted by the Data Fiduciary.

The offer and acceptance documents are authenticated to make them admissible in a Court of law either by the use of a valid digital/electronic signature or through a certified form of electronic document (eg: Certificate under Section 65B of Indian Evidence Act in India).

Alternatively, the offer and acceptance need to be authenticated with the collection and retention of such meta data that would be acceptable in a court of law as reasonable evidence of the free consent having been obtained.

When personal information is collected directly from the data principal in consideration of any service offered, the consent is recorded before the processing of the personal data and conforms to the requirements of a comprehensive notice which highlights the principles of processing, the rights of the data principal including the right of withdrawal of the consent, the form of grievance redressal etc. This contains the disclosure of the purpose of collection, details of the type of information collected, the retention period, cross border transfer if any, transfer to other co-data fiduciaries or data processors etc. as covered by the basic "Purpose Specific Privacy Policy" of the organization.

When a data principal expires, the status of the data principal and the compliance obligations change. In some data protection regulations, the applicability of the compliance obligations may continue for a period after the death of the data principal (Eg: Singapore law where the definition of a natural person extends to deceased persons and the obligations of personal data protection extends to 10 years after death).

When the lawful basis for collection and processing of personal data is "Consent", the death of a person (as well as loss of contractual capacity such as insanity or insolvency) immediately terminates the contract. Hence the "Consent" no longer remains valid. Additionally if the law is meant to protect the privacy right of a living natural person, the applicability of the law also ceases.

Any instruction of a natural person regarding disposal of the information after his/her death is a testamentary document (like a Will) and in some laws (eg Indian Information Technology Act 2000), an electronic document which is testamentary in nature is not recognized in law.

Hence the consent obtained before the death of a data principal will be invalid on the receipt of the notice of death by the Data Fiduciary. The personal data collected under such invalidated consent no longer has the status of the protected personal data as per the subject data protection law.

Such information is also not in the form of "Anonymized" personal information since it may still contain the individually identifiable parameters and hence cannot be considered equivalent to "Non Personal Information".

Since most of the data protection laws are not clear about how to deal with such "Personal data of Deceased Data Principal" (PD-DDP), this addendum policy is created as an extension of the Purpose specific Privacy Policy and covers the identification, continued use, archival, deletion etc of the personal data of deceased data principals including "Suspected deceased data principals".

Policy

Discovery of PD-DDP

1. The organization makes a reasonable effort to scan the public information available in cyber space to identify if there is any knowledge about the death of an individual whose personal data may be available in their repository.

   A search of publicly available obituary data or data which may indicate the possible instances of death of data principals whose personal data is in the custody of the organizations is conducted at regular intervals (not exceeding one month) to identify potential sets of personal data of deceased persons in the repository of personal data in the custody of the organization.

   Such identified information is classified and flagged as "PD-RDDP". (Personal Data of reportedly deceased data principal).
2. The organization under its "Purpose Specific Privacy Policy" (PSPP) sends a personal data confirmation request once every year to the last known e-mail of the data principal requesting confirmation of the current version of the PSPP. In the event no reply is received within 7 days of the receipt of such a notice or if the email bounces for reasons such as "No Such account exists", the consent confirmation is escalated to the next level of confirmation where a reminder is sent through another mode of communication if available (eg: SMS through mobile). If no response is received for this message within 2 days, the request for consent is escalated to the third level where a notice is sent to the individual in at least two modes of communication that the account will be placed under suspension unless the confirmation is received within 24 hours.
3. In the event no response is received, the case is referred by the DPO to the Data Governance Committee recommending transfer of the personal data to a "Dormant-Suspected deceased status". The continued use of such data will depend on existence of any legitimate interest of the organization including the need to account for any financial transactions between the organization and the individual. Such data would be transferred to a secondary data storage space and would be subject to a higher level of security.
4. Where there is no legitimate interest in continuing the processing of the data, dormant data would be archived in an encrypted state and not processed further in the normal course. Any subsequent request for access shall be treated as an "Incident" and resolved with appropriate verification and authentication by the DPO.
5. Where the personal data remains dormant for more than 2 years, the data shall be further tagged as "Inoperative-Strongly Suspected deceased" status and moved to a tertiary archive of such data which is encrypted. Any subsequent request for access

shall be treated as an "Incident" and resolved with appropriate verification and authentication by the DPO.

6. Where the personal data remains in-operative for more than 5 years, the "Consent prohibiting disclosure" is considered as in-operative and a notice shall be published in a Cyber notice service such as "Cyber-Notice.com". After a further period of one month, if no claim for the information comes from either the data principal or any legal representative, a notice is sent to the Data Protection Authority or any other designated authority that the data may be transferred to their custody for further archival. In the event the authority refuses to receive such data, the data may be deleted or anonymized and converted into Non Personal data.
7. Any time after an account is flagged "Dormant", the Data Fiduciary shall endeavour to identify the legal heirs of the suspected deceased data principal and initiate a claim process from their end.
8. Where the data fiduciary has a data asset of the data principal in his custody and money is being received as royalty or otherwise and an attempt to make payments to the data principal fails because the transaction bounces or the receiving banker refuses to collect the amount for any reason (even without confirming the death of the account holder), the accumulated asset and money is considered as held in trust for the Data Fiduciary and his legal heirs. The money in such accounts shall be kept in the form of a special reserve of "Unclaimed Balances" with the data fiduciary.
9. Where the data fiduciary receives a confirmation of death, the information is verified through appropriate means and the known legal heirs are notified directly and through Cyber notification to file their claim for settlement as per procedure outlined below. Pending settlement of the claim a new tag of "Under Claim Settlement Process" is assigned to the data set and shall be moved into a data vault with appropriate security in terms of encryption and access control. When the claim is settled, the information is released to the successful claimant after holding a copy thereof for contingent requirement for a further period of 180 days after which it may be deleted.
10. After a personal data is classified as "Inoperative" and appropriate public notice through Cyber Notice system is served for which no response is received, it is considered that the data fiduciary assumes a legitimate interest to process the information as per this policy.
11. In order to facilitate the claim process in case of death, every account holder is provided with an option to nominate an "Alternate" e-mail ID or a designated nominee who would be considered as a virtual representative for the purpose of managing the account after the death of the data principal.
12. For Indian data principals, an option would be provided to the individual to deposit the instructions on how to handle the account after death of the data principal through a letter in writing since "electronic Will" is not recognized in India. The physical letter would be considered as the original instruction and the e-mail will be an electronic copy. The physical letter would be archived without opening and only when the report of the death of the deceased person is received, it would be opened to confirm the electronic instruction.

Claim Settlement Process

1. A legal heir of a deceased data principal may approach a data fiduciary on knowing that the deceased data principal had an account with the data fiduciary such as an E Mail account or a Drop Box account etc where some valuable personal data or data which belonged to the deceased person (including non personal data) may be present.

2. He/she would not be having the password to the account and even if he had the password, it would be incorrect for him to log in in the name of the deceased since it would amount to impersonation under law.
3. Further the property of a deceased person may belong to several legal heirs and unless the deceased has nominated an individual to receive the property for the purpose of re-distribution.
4. The legal heirs would be required to file a joint claim declaring themselves to the only surviving heirs of the deceased who died intestate as to the said digital property. The letter signed by all shall be supported by an eKYC based on Aadhaar or by a Bank Manager or a Court order.
5. The Claim process would be charged a nominal fee of Rs 1000/- or such other fee that the Data Protection Authority may determine as a reimbursement of expenses.
6. On receipt of a valid claim, the Data Protection Committee shall approve the disclosure of the information to the claimant/s and archive the data for a period of further 180 days as a contingent back up.
7. After the expiry of the 180 days cooling time, the data may be destroyed.
8. In the event the data has already been transferred to the Data Protection authority the claim may be diverted to the appropriate authority for further action.

Any dispute arising out of this policy shall be resolved with online mediation and/or arbitration through DDMAC. (Data Disputes Mediation and Arbitration Center of FDPPI) or through the Adjudicator under the personal Data protection act.

Report by the FDPPI Internal Committee on Handling of Data of Deceased Data Principals

FDPPI had set up an internal committee of or members headed by Dr Mahendra Limaye (Advocate) on Data Privacy of deceased individuals and has submitted its report reproduced here.

Ms Meena Lall, Abhay Warik, Shalini Varanasi and Subburayudu Tallapragada and others have also contributed to the report as members of the Committee.

The copy of the report submitted by the Committee is enclosed.

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

A Report submitted by the FDPPI committee under the Chairmanship of Dr Mahendra Limaye

Data Privacy Rights of Deceased Individuals

An individual would wish to keep their privacy intact even after their departure from the world, as certain disclosures could adversely affect:

- their otherwise carefully maintained dignity during their lifetime or
- the privacy of their family members or
- the privacy of their other connections.

Can we therefore say that data privacy rights should be afforded to the individuals even after their expiry and to what extent? Let us examine the world view to understand if a standard operating procedure can be suggested in this regard.

Applicability of Data Protection Laws to the Personal Data of Deceased Individuals – Worldwide View

A very few Data Protection laws have mentioned the personal data of deceased individuals as part of the law, that too - either to highlight the exclusion or to specify the limited scope of applicability of the provisions. Sharing some examples in the table below:

GDPR
According to the Recital 27 of the GDPR, the Regulation ***does not apply*** to the personal data of deceased persons and EU Member States may provide for rules regarding the processing of personal data of deceased persons.
Spain (GDPR)
The SDPA ***does not apply*** to the personal data of deceased individuals. However, Article 3 provides that ***heirs are entitled to access, request deletion and rectification of the relevant data*** from data controllers and processors, unless

deletion or rectification was prohibited by the deceased individual or by applicable law. Executors can also act as heirs. If an heir is a minor or disabled then the ***Public Prosecutor*** can act on their behalf.

(Source: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/deceased-persons)

Italy

Section 2-terdecies of the IDPA provides that the rights referred to in Sections 15 to 22 of the GDPR for deceased people ***can be activated***:

- by a data subject who has an interest in the protection,
- by his agent, or
- for family reasons worthy of protection ("Representative")

The exercise of the subject's rights by the Representative is ***not allowed*** in the ***cases set out by law*** or when, the ***data subject has expressly forbidden*** it with a written declaration provided or communicated to the data controller.

(Source: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/deceased-persons)

DP Act, UK

According to ICO guidance, the DP Act applies to information which relates to an identifiable living individual. Information relating to a deceased person does not constitute personal data and therefore is not subject to the UK DP Act.

PDPA, Singapore

The PDPA defines an individual as “a natural person, whether living or deceased”.

Accordingly, the personal data of deceased persons ***is protected*** under the PDPA. However, it does not apply to the personal data about a deceased individual who has been dead for more than 10 years.

The ***organisations are expected to take note*** of the individuals who may act on behalf of the estate of the deceased individual in respect of matters relating to the deceased’s personal data.

Also, PDPA applies to ONLY a limited extent in respect of the personal data of deceased individuals, i.e., only the provisions relating to the disclosure and protection of personal data will apply.

The abovementioned ***‘limited extent’*** covers:

- Notification of purposes for disclosure of personal data
- Obtaining consent for disclosure of personal data
- Disclosing personal data for purposes which a reasonable person would consider appropriate in the circumstances
- Making a reasonable effort to ensure the accuracy and completeness of personal data that is likely to be disclosed to another organisation
- Making reasonable security arrangements to protect personal data

This is intended to minimise any adverse impact of unauthorised disclosure of such data on family members of the deceased.

While the PDPA does not apply to personal data of individuals who have been deceased for more than 10 years, there may still be ***other legal or contractual requirements*** that organisations should be mindful of.

Out of the above examples, Singapore PDPA provides the most comprehensive provision on the handling of the personal data of the deceased.

Applicability of PDPB 2019 to Personal Data of Deceased Individuals

PDPB defines a "data principal" as *the natural person to whom the personal data relates*. The definition of data principal itself keeps the deceased individual's data out of the scope of the law.

During the lifetime of the Data Principal, the Data Fiduciaries are required to process the personal data as per the Data Protection Laws and provide for certain rights. In order to understand whether the deceased individual's personal data can be lawfully processed, it becomes important to understand the lawful purpose originally relied on by the Data Fiduciary.

Under section 4 of PDPB, *no personal data shall be processed by any person, except for any specific, clear and* ***lawful purpose***. Ensuring the Lawfulness of processing is the first obligation under PDPB which Data Fiduciaries must comply with. Hence, companies need to ensure to have a lawful basis before processing any personal data and PDPB provides different lawful bases for processing.

Let us explore under what circumstances a Data Fiduciary can continue processing personal data of deceased Data Principal(s).

1) **Where Personal Data is processed as per Section 12 – PDPB 2019 - Grounds for processing of personal data without consent in certain cases:** In these cases, the processing may continue as required under the applicable law. For example, in case an order or judgment of any Court or Tribunal in India requires processing of personal data of the deceased, the Data Fiduciary will have to continue storing/providing the information as may be instructed by the Court/Tribunal.

2) **Where the Personal Data is processed as per Section 13 – PDPB 2019 - Processing of personal data necessary for purposes related to employment, etc.:** It is reasonable to conclude in this case that the Data Fiduciaries can continue to process the deceased employee data for the closure of the contract and to fulfil other legal obligations.

3) **Where the Personal Data is processed as per Section 14 – PDPB 2019 - Processing of personal data for other reasonable purposes:** The processing of personal data of deceased individuals will not be lawful in this case, since the Data Fiduciary is required to take into consideration the reasonable expectations of the

data principal having regard to the context of the processing. Which will not be possible to judge and consider in the cases of deceased data principals.

For the purpose of discussion on Data Privacy rights of the deceased we have limited the scope to the scenarios where *the consent is used as a lawful basis* for processing. Since, as briefly discussed above, under other lawful bases, the Data Fiduciary and the Data Principal may find ways to lay down the standard terms for treatment of personal data or digital assets of the Data Principals or the Data Fiduciary might have to process the data under a legal obligation to cover the lawful basis.

4) **Where Consent is used a lawful basis (Section 11, PDPB 2019):** Under section 5 of PDPB, *every person processing personal data of a data principal shall process such personal data— (a) in a fair and reasonable manner and ensure the privacy of the data principal; and (b) for the* ***purpose consented*** *to* ***by the data principal*** *or which is* ***incidental to or connected with such purpose****, and which* ***the data principal would reasonably expect*** *that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.*
Section 5 puts it very clearly that the purpose must be consented by the data principal, therefore, in the absence of the consent the processing will become unlawful. Similarly, when consent is withdrawn by the data principal, the Data Fiduciary is obliged to stop the processing.

Since, in the case of a deceased data principal, the consent will lose its validity and therefore, in effect like withdrawal of the consent, the Data Fiduciary will be obliged to stop the processing.

It is very important to highlight here the **Role of a Consent Manager** in case the Data Fiduciary chooses to avail the service.

Under section 21 (1) of PDPB, *the data principal, for exercising any right under Chapter V, except the right under section 20 (Right to be forgotten), shall make a request in writing to the data fiduciary either directly* ***or through a consent manager*** *with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.*

For the purposes of this section, ***a "consent manager" is a data fiduciary*** *which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.*

Therefore in effect, the consent managers will be merely acting as agents for the data principals and the rights applicable under the law will become ***non exercisable by the consent managers*** as well, upon the demise of the data principal, since the contract between the two parties will become void.

Further, the consent managers as Data fiduciaries will also have to stop the processing of personal data of the deceased individuals and in turn inform the other

data fiduciaries processing such data based on the consent shared and managed by them.

Discontinuing the processing here includes data deletion from the records of the data fiduciaries including from the records of the consent managers (as independent Data Fiduciaries).

As far as the consent managers as data fiduciaries are concerned, the law PDPB) provides them with just as many rights as authorised by the data principals during their lifetime and limited to the scope of rights relating to the data principals. They do not become owners of the personal data of the data principals in any manner. Moreover, the right to be forgotten also remains exercisable by the data principal alone and cannot be exercised via a consent manager even during the lifetime of the Data Principal.

Now, the question arises that since the PDPB 2019 does not apply to the personal data of the deceased individual, can the Data Fiduciaries continue to use the data in case they continue to find the data as commercially useful to further their business. For example, in case a Facebook page of a deceased individual continues to attract advertisers with successful viewership, can they continue to use the existing personal data with them (Facebook), assuming in this instance that Facebook has not laid down any policy on its own.

Suggestion: PDPB can introduce a provision to enable establishment of instructions by the Data Principals during their lifetime for the management of their personal data after their demise.

In such case, it will become convenient for the Data Fiduciaries to lawfully handle the deceased personal data. Of course, such disposal will have to be in accordance with the other applicable laws.

Further, the data principals will be able to decide and share the instructions during their lifetime about to whom they would want their data to be transferred for further use/disposal. The Data Fiduciaries will just need to transfer the data to the other individual(s) as instructed (this can be limited by considering the technical feasibility and any potential harm to the business interests) and thereafter dispose/handle the data keeping in mind the data retention obligations under other applicable laws.

Different Scenarios: where guidance would be useful – Data Fiduciaries offering different services

Can Data Fiduciaries be expected to monitor the digital assets of deceased data principals in their possession or any information in their access that can be used as a tool to gain ownership of other assets of deceased data principals including digital, financial as well as physical assets? And can they be expected to monitor their disposal after the demise of the data principal?

In the cases of Data Fiduciaries that process personal data to provide for certain services wherein the access to the data stored on their systems is controlled by the users. The personal data processed by them in effect remains limited, however, because of the nature of the

services provided the data stored and managed by the user could amount to a great deal of personal data or digital assets. For example, email and cloud storage services.

As far as data protection laws are concerned, the data fiduciaries are legally bound to process the personal data as per the laid-out data protection principles which include purpose limitation and data retention restrictions. Therefore, once the Data fiduciary comes to know about the demise of the data principal, they would need to *either restrict or stop the processing depending on the lawful basis relied upon for the processing.* Also, they will have to either delete the data as required under the data protection laws or retain it away from the live environment as may be required under any other applicable law to the Data fiduciary.

It is important to highlight here that the Data Fiduciary obligations as per Data Protection laws is limited to the personal data collected and processed by the Data Fiduciary. Therefore, the data stored in the Data Principal's control remains their own responsibility. Considering this, in case the Data Principal is storing valuable digital assets using the Data Fiduciary's services - after the demise of the individual, the access to the assets by the legal heirs may become a lengthy and drawn-out legal process if no guidelines are set in advance.

For example, as per the Yahoo Email's Terms of Service upon receipt of a death notification along with a copy of the death certificate, the user account is terminated and all contents therein are permanently deleted. Also, the access to the account is non-transferable. Now, in case the legal heirs have reasons to believe that the email account could be holding potentially valuable information, to access they will have to go through a legal process to question the Terms of Service in order to gain access to the account.

Yahoo Email (Excerpt from Terms of Service)

No Right of Survivorship and Non-Transferability. You agree that your Yahoo account is non-transferable and any rights to your Yahoo ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.

(Source: https://policies.yahoo.com/sg/en/yahoo/terms/utos/index.htm?redirect=no#:~:text=You%20agree%20that%20your%20Yahoo,all%20contents%20therein%20permanently%20deleted.)

On Comparison, for example, we can see that some of the Data Fiduciaries could on their accord, make the Data Principals aware that they could leave instructions during their lifetime about how to manage their data. For example, sharing an excerpt from Google Account Help.

GMAIL (Excerpt from Google Account Help)

People expect Google to keep their information safe, even in the event of their death.
***Make plans for your account** - 'Inactive Account Manager' is the best way for you to let us know who should have access to your information, and whether you want your account to be deleted. Set up 'Inactive Account Manager' for your account.*
***Make a request for a deceased person's account** - We recognize that many people pass away without leaving clear instructions about how to manage their online accounts. We can work with immediate family members and representatives to close the account of a deceased person where appropriate. In certain circumstances we may provide content from a deceased*

user's account. In all of these cases, our primary responsibility is to keep people's information secure, safe, and private. We cannot provide passwords or other login details. Any decision to satisfy a request about a deceased user will be made only after a careful review.
(Source: https://support.google.com/accounts/troubleshooter/6357590?hl=en)

Now, depending upon the services offered the nature of personal data and the disclosure reach can differ. Also, in absence of guidelines, the Data Fiduciary might exercise control over the Data Principal's data post his/her demise. For example, Facebook memorialises the account on being made aware that an individual has passed away which does not require submission of documents by a legacy contact. Only in case of a request for the deletion of the account certain documents are required to be submitted. Making the Data Principal aware and allowing them to leave instructions about management of their account post their demise would be a good privacy by design policy.

Facebook (Excerpt from Help Centre - Policies and Reporting)

If Facebook is made aware that a person has passed away, it's our policy to memorialise the account. Memorialised accounts are a place for friends and family to gather and share memories after a person has passed away. Memorialising an account also helps keep it secure by preventing anyone from logging in to it.
If you're a legacy contact, learn how to manage a memorialised account. If you'd like to report a deceased person's account to be memorialised, please contact us.
How do I request the removal of a deceased family member's Facebook account?
The fastest way for us to process your request is for you to provide a scan or photo of your loved one's death certificate.
If you don't have your loved one's death certificate, you'll need to provide proof of authority and proof that your loved one has passed away. Please see the documents that we accept below.
Submit one document to provide proof of authority:

- *Power of attorney.*
- *Birth certificate.*
- *Last will and testament.*
- *Estate letter.*

Submit one document to provide proof that your loved one has passed away:

- *Obituary.*
- *Memorial card.*

Once you have the required documentation, please send us a request.

(Source: https://www.facebook.com/help/275013292838654/?helpref=hc_fnav)

Going by Apple's policy, they provide assistance in accessing deceased person's information ***only*** after ***a court order*** is obtained and is presented by the deceased's next of kin to prove rightful heirship.

Apple Account (Excerpt from Apple Support - How to request access to a deceased family member's Apple accounts)

In the unfortunate event of a customer's death, Apple will not be in a position to know if they would want their information to be shared with anyone or with whom they might want to share it.
Before Apple can provide assistance in accessing a deceased person's device or the personal information they stored in iCloud, we ask that the person's next of kin obtain ***a court order*** *that names them as* ***the rightful inheritor*** *of their loved one's personal information.*
We ask that the court order specify:

- *The name and Apple ID of the deceased person.*
- *The name of the next of kin who is requesting access to the decedent's account.*
- *That the decedent was the user of all accounts associated with the Apple ID.*
- *That the requestor is the decedent's legal personal representative, agent, or heir, whose authorization constitutes "lawful consent."*
- *That Apple is ordered by the court to assist in the provision of access to the decedent's information from the deceased person's accounts.*

If you have a court order with this information, or if you need additional help, please contact Apple Support.
We have great sympathy for surviving family members. Once the court order is received, we will help as much as possible to grant access to the personal information or devices you are requesting. Please note that devices locked with a passcode are protected by passcode encryption, and unless the next of kin knows the device passcode, Apple will not be able to remove the passcode lock on the device without erasing it.
About estate planning
We encourage customers to add an inheritance plan to their will that covers the personal information they store on their devices and in iCloud. This may simplify the process of acquiring a proper court order and reduce delay and frustration for family members during a difficult time.
(Source: https://support.apple.com/en-us/HT208510)

It is clear that the Data Fiduciaries are well aware of the legal obligations under the Data Protection Laws and they would not want the data privacy rights to be transferable and in turn become perpetual obligation for them even after the use-case comes to an end post the demise of the Data Principal. Therefore, to bring the disposal of the personal data of the deceased individual to a logical closure, an obligation defined by the law can be a solution to set the reasonable expectations from the Data Fiduciaries.

THE RIGHT TO INFORMATION IN THE PROPOSED PRIVACY REGIME

M G. Kodandaram

Right to Information Act, 2005 – the need

Democracy is primarily a political system that is meant for providing freedom of various forms to the residents with a view to provide positive social environment necessary for a happy living. Freedom to speak and express with reasonable restrictions is one of the most cherished basic human needs that plays a vital role in enhancement of individual's personality. In a democracy like India, all the citizens have a fundamental right to be informed about the ways and manners in which they are being governed by the Public Authorities (hereinafter PAs), in a transparent and timely way, so that such informed citizen could point out shortcomings in governance so that the same could be addressed and set right. In a vibrant democracy, citizens are the rulers and also are the ruled, both the king and the servant at the same time.

The Article 19 of the Constitution pledges the citizen 'the right to freedom of speech', which is essential in the evolution of a healthy informed Society. In Bennett Coleman & Co. v/s Union of India (AIR 1973 SC 106), striking down the validity of the Newsprint Control Order that fixed the maximum number of pages to be printed by a newspaper publisher, the Hon'ble Supreme Court held it to be violative of provision of Article 19(1)(a). The Court observed that the freedom of the press was an essential element of Article 19(1) (a) and has to be regarded as a critical element in freedom of expression. The Apex Court in the case of State of U.P vs. Raj Narain (AIR 1975 SC 865) held that 'the right to know' is a right inherent in Fundamental Right to freedom of speech and expression guaranteed under Constitution. Similarly, in the case of Peoples Union for Civil Liberties vs. Union of India, ((2004) 2 SCC 476) and in plethora of cases, the Supreme Court observed that Right of information is a significant facet of the freedom of 'speech and expression'. This makes 'Right of information' indisputably a fundamental right which has been asserted and recognized by the judiciary from the time of adoption of the Indian Constitution.

It is true that an informed citizenry and a transparent administration are vital for the effective and successful functioning of any Government in a country. Unfortunately, it has become a bad practice on the part of PAs, whenever any information is called for by the Public, to take their own time in providing information or even abstain from providing such information citing some reasons. Such routine lapses in services by the PAs would go unabated, if there are no fair mechanisms and punitive policies in place to obtain timely information from such Authorities / Departments. However, there is always a remedy available to the citizen, which is to approach the courts to direct such PAs to furnish the solicited information. At the same time, it is true that it is not feasible for a citizen to approach the judiciary at every time to seek directions/orders to make the PAs render such information. Further the judiciary are neither prepared nor expected to handle such voluminous requests that are bound to arise, as the current state of pendency in various judicial forums indicate. Therefore, to bring in a

practical regime wherein the citizen could access information from PAs within a timeframe in a definitive way, the Indian Parliament enacted the Right to Information Act, 2005 ("RTI") which came into force from 12th October 2005.

Objectives of RTI Act

The purpose of the enactment, as declared in the preamble, is to provide the necessary legal framework for setting out the practical regime of right to information for citizens to secure access to information under the control of PAs, in order to promote transparency and accountability in the working of every Public Authority and to constitute a Central Information Commission and State Information Commissions for to oversee the implementation part. The main objectives of the RTI Act are: (i) to set out a practical regime of right to information for citizens; (ii) to secure access to information under the control of PAs; (iii) to promote transparency & accountability in the working of every Public Authority; (iv) to contain corruption in Public services; (v) to increase the awareness & ability to exercise their other rights by the citizens; and (vi) to equip them to participate meaningfully in the development process.

However, the revelation of information in actual practice is likely to conflict with other public interests like the preservation of confidentiality of sensitive information and therefore it is necessary to harmonise such conflicting interests while preserving the paramountcy of the democratic ideal. The RTI act is expected to synchronize such conflicting interests so as to protect the fundamental rights with reasonable restrictions in place as per Article 19(2) of the Constitution. From the above legal position, it can be concluded that RTI Act is a powerful tool that can deliver significant social benefits, provide a strong support to democracy, promote good governance by empowering the Citizen's ability to participate effectively in governance of the country and also hold the Public Servants accountable.

Meaning of Right to Information

As per Section 3 of RTI Act, 2005, all the citizens shall have the Right to Information. The 'information' under the act means any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force[Sec.2(f)], and the right is to have access to such information held by or under the control of any Public Authority including the right to (i) inspect the work, documents, records; (ii) take notes, extracts or certified copies of documents or records; (iii) take certified samples of material; (iv) obtain information in the form of diskettes, floppies, tapes, video cassettes or in any other electronic mode or through printouts where such information is stored in a computer or in any other device.[Sec.2(j)]. The PAs covered under the Act are any authority or body or institution established or constituted, (a) by or under the Constitution; (b) by any other law made by Parliament; (c) by any other law made by State Legislature; (d) by notification issued or order made by the appropriate Government, and includes any, (i) body owned, controlled or substantially financed; (ii) non-Government

organization substantially financed, directly or indirectly by funds provided by the appropriate Government [Sec.2 (j)].

As stated above the RTI act with a purpose to harmonize certain conflicting interests, including such matters relating to personal information of an individual which would cause unwarranted invasion of the privacy of such individual, has exempted disclosure, which act as reasonable restriction, as available under article 19(2) of the Constitution.

Privacy Concerns of an Individual

In any democracy the 'Right to Privacy of an individual' is a much desirable right. The protection of the Personal information of an individual has become more challenging in these days, as all the entities, including PAs involved in various activities and services are collecting personal data of individuals for various purposes. Such personal information aggregated with a view to extend better services could be exploited by fraudsters through illegitimate channels and if there are no fair law in place, it could be used by them to commit diverse crimes. The rampant deployment of digital technology tools to collect such personal data, without the consent or knowledge of the subject, has created a scary situation for the privacy rights of an individual. When such personal data reaches the dark nets dominated by outlawed criminals, the damage it could cause to personal life and liberty of such individual cannot be guesstimated.

One may wonder as to why, at present, so much of importance is given to the protection of privacy rights? Personal information and privacy concerning such information are as old as mankind, but not much attention was given to such rights in the past. From the last 2 or 3 decades citizens around the globe are demanding the status as fundamental rights to the personal information so as seek paramount protection from breach of privacy that is critical to their very survival. The changed social condition and circumstances to which the netizen is driven to make such claims, could be pointed out to the reasons deliberated in the following part.

Increased Crimes in Cyber Space

In earlier times the flow of any information was in snail's pace. Most of the times, the information could be passed on by word of mouth and in some critical situations, through runners for urgent communications. As days passed the various scientific inventions and means of improved ways of communication, including the telecommunication technology brought more paces to these activities, but still, certain barrier could be laid down in law and practice, so as to prevent the flow of information to the hands of Criminals. Further most of the activities were carried out in the physical presence of individuals, which had some kind of legal measures to prevent any misuse of such information. The technology of the current age viz., Information Communication Technology (ICT) has turned out to be disastrous as for as control of flow of personal information are concerned, as it is not in a position to prevent harm caused to individuals and the social fabric of the human settlements. The use of mobile technology as well as increase in the density of smart phone users in India has further aggravated and accelerated the criminal activities in the cyber world.

The digital technology, the 'global common' accessible to the entire population, has no respect for territorial or political sovereignty, with little restrictions in place. This sort of technological explosion has given way for rampant information exchange and the related activities between citizens of different locations and Nations. These changed circumstances have resulted in a situation where the personal data of an individual could be gathered remotely and exploited for meeting the ulterior motives by the cyber criminal or the enemy Nation within fraction of minutes. The dynamic development of computer technology and increase in volume of internet users around world, has threatened the society and people concerned due to increased cyber-crimes, which have assumed gigantic proportions. These changed circumstances have given rise to an entirely new set of challenges to the law enforcement agencies all over the world as the existed laws which are useful during traditional times are no more suitable or apt in the new cyber world. The laws made by the Nations are territorial in nature but the crimes committed are universal. The usage of digital technology, open for participation by all and accessible to the entire population without any obstruction or restrictions has driven the society to a peculiar situation where the personal information require a different standard of protection to avoid damages and harms in the hands of fraudsters and their network. As on date, any information could be shared with the whole world in a flash and this has caused a huge embarrassment and injury to individuals in respect of protecting their personal information, which are essential for a peaceful living. By showing complete disregard and disrespect for the moral and national values with scope for anonymous and pseudonymous application, the world's biggest information network has turned out to be a paradise for the criminals. The perpetrators of crime, residing in any part of the globe could cause huge harm and damage to an individual's reputation, wealth and mental health exploiting the current technology to their advantage. The victim may not be in a position to know who the criminal is and from where such wrongs are being carried out. Even the law enforcing authorities are in a state of worry as the existing laws and the international situation do not assist them even a bit to safeguard the interests of the victim and of the society in general. It has equally become a cause of serious concern to every user, to find effective ways and means to prevent and combat the unregulated illegal flow of data worldwide. In view of the changed circumstances and free flow of information in a break neck speed, there is phenomenal increase in cyber-crime followed by Cyber terrorism and Cyber war in the present society. There are state players encouraging and backing such criminal activities which cause a huge threat to the entire mankind. Therefore, there is urgent need for suitable privacy protection laws to enforce discipline, transparency and accountability for aggregation and usage of personal data in India and across the world, so that such cyber-crimes could be identified, contained and the victims could be sufficiently protected and saved.

The changed situation could be better understood by the following illustrations.

(a) Any private health information which is critical to individual and their family, and to the hosptal, could reach the whole world in no time. The criminals could pounce on such information to commit various types of crimes. This is more evident in these days of pandemic

where the fraudsters are using it for harming the reputation. They engage themselves in many illegal activities, starting from spreading of fake information, to outright exploitation of money by distressed public in varieties of ways, and up to causing of internal disturbances within the society and Nation. The famous toolkits employed to dishonor nations are such instances which needs to be contained. When information flow is without geographical and sovereign barriers, how one could have a peaceful natural survival and happier living? Therefore, the primary requirement of the present situation is to protect the personal information of an individual as a basic fundamental right.

(b) The banking and financial transactions of an individual in the earlier era could not have caused much heartache to the individual in the traditional ways. The physical presence was essential to carry out any financial transactions. When this is compared to the present day of digital banking, any details about an individual or entity entering the public domain may end up in entire account being emptied in no time by the fraudster. The digital technology has put forth such a situation that as an individual, one had to protect details of one's account, date of birth, ATM card number, Aadhaar number, internet banking passwords etc., so as to protect the property being looted. Added to this the rampant use of crypto currencies with no legal backing and accountability has created a heaven to the transactions by criminals which may even result in destabilization of financial and economic conditions of a nation. These have turned out to be Super–ponzi duping centers, resulting in loot of money through illegal trade and commerce in prohibited goods and services which are a threat to society and environment.

Laws in Place for Privacy Protection

As on date, there are no specific laws for the protection of personal data of an individual in India. The Information Technology Act 2000, (IT Act) the primary legislation that regulates the ICT products and the usage of the data in electronic format has limited scope for protection of Personal information of individuals by the corporate engaged in the data related activities. The IT Act framework, in addition to regulation of the electronic applications, storage, processing, authentication as well as electronic contracts, e-commerce, cyber offences and liability of network service providers, also provides protection in respect of digital data or information concerning the privacy of an individual. The Sections 43, 43A, 72 and 72A of the IT Act read with "The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) (SPDI) Rules 2011 is the specific provision as on date that covers the matters relating to 'sensitive personal data' and protection of such data. The Section 43A and the SPDI Rules apply to 'body corporate', requiring them to maintain reasonable security practices and to follow the due diligence principles while possessing, dealing or handling data in a computer resource. In view of the general protection provided under this law, one can conclude that the IT Act does not exclusively deal with the 'right to privacy'. As stated in the earlier part, the cyber space has been exploited by the criminals to the core and law enforcement agencies finding it impossible to combat against such unregulated illegal flow of personal data.

Privacy – Now a fundamental right

The need for a personal data protection law in India attained urgency and significance, when the government started the 'Aadhaar project' which aimed at building a database of personal identity and biometric information covering every Indian resident. As on date the registration of a person under Aadhaar has become inevitable activity as this information is mandatory for filing tax returns, for opening bank accounts, for securing loans, for buying and selling of property and many more similar transactions. If such critical personal data goes unprotected, it will cause huge harm to the individual, the society and the country.

In view of the changing circumstances where breach of personal information flowed without any barriers, the Supreme Court of India, in the case of Justice K.S. Puttaswamy v/s Union of India [(2015) 8 S.C.C. 735 (India)], passed a historic judgment on 24th August 2017, affirming the constitutional right of a citizen to protect her / his personal data so as to preserve the privacy. The Article 21 of the Constitution mandates that, "No person shall be deprived of his life or personal liberty except according to procedure established by law". The Apex Court held that the right to privacy is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights, securing individual's liberty. Further the individual's dignity is cited as a basis for extending it the status for personal information as a fundamental right. Further, the Supreme Court, clarifying that the 'right to privacy' is not an "absolute right", allowed reasonable restrictions in certain situations subject to conditions, such as (i)there must be existence of a genuine state interest; (ii) such restriction should be proportionate to the interest;(iii) and it shall be through valid legislations.

The Indian government announced the appointment of an expert committee headed by Justice (Retired) B N Srikrishna to devise a legal framework for protection of personal information and data. Further, based on the report by the experts, the Government introduced 'The Personal Data Protection (PDP) Bill, 2019' in the LokSabha on December 11, 2019, which was referred to a joint parliamentary select committee for scrutiny. The JPC has since submitted the report and the recommended bill is pending consideration of the Government and the Parliament.

RTI Act and PDP Bill Interplay

From the above legal position, it seems that the purpose and objectives of RTI Act and PDP Bill are acting in opposite interests and directions. The former provides the right to information held by a Public Authority by any citizen, whereas the latter, allows an individual to guard her/his personal information from reaching the public domain. To have a fair analysis of the legal realms, it is important to examine as to how the privacy issues are protected in the RTI regime, the limitations and safeguards provided to privacy matters so as to find out the legal measures for the privacy of an individual to receive the deserving protection in both the enactments and circumstances.

Before proceeding for a detailed examination, it is better to understand certain common issues in order to have meaningful discussions. Both the legal exercises are from the Parliament, applicable to the whole of India. The RTI Act is principally built around Article 19 of the Constitution and the PDP Bill, on Article 21, and both are guaranteed fundamental

rights that deserve equal merit. However, both the rights are not absolute rights as reasonable restrictions could be carved out through proper legislations. The RTI Act predominantly covers and concerns the PAs whereas the PDP Bill encompasses all fiduciaries and processors, including the PAs. The types of data collected by PAs include the personal data, collected in fiduciary capacity or otherwise, as well as non-personal data. Both the legislations have provisions for formation of authorities, namely the Central Information Commission (CIC) and State Information Commissions (SICs) for administering RTI Act and data protection Authority (DPA), to oversee the compliance and implementation of the law and procedures in the making. The personal information in any form like, in traditional paper-pen mode or digital mode, needs the necessary protection so as to protect the rights of the individual. Further the terms like 'Personal information, 'Fiduciary, though find place in the enactment, are not defined in the RTI act.

RTI Act Protects the Personal Information

As stated earlier the right to information is not an absolute right. Therefore the information that the Public Authority generates are to be given to the public, subject to reasonable restrictions stipulated under the said act. There are various categories of information, which are sensitive in nature that if released to the public, might actually cause serious Injury to either other's rights or to the effective governance etc., For example, during conflicts, if an applicant seeks information regarding troops movement or deployment, the Government needs to protect such details as secret in the larger interest and safety of citizens. Similarly, if someone asks for personal information about another individual which are sensitive in nature, such information may not be in the interest of that individual or the public and may be subjected to harm by the applicant or recipient of such information and the same needs to be denied. The exemptions to requests for information under the Act are primarily covered in three sections viz., the Section 8, Section 11, and section 24. The Section 8 lists nine specific exemptions ranging from sovereignty of India to personal information. The Section 11 provides protection to confidential third-party information. The Section 24 exempts certain security and intelligence organizations from the purview of the Act. If the information sought by an applicant falls under any of the exempted categories of information, the Public Authority must offer the reasons for rejection of requests.

The Section 8 (1) of the RTI Act being a non-obstante clause overrides other provisions of the RTI Act. The excerpted part of the section 8 of the RTI Act, relevant to our discussions on privacy of an individual, is reproduced hereunder:

"Sec 8. (1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen, -

(e) Information available to a person in his fiduciary relationship, unless the competent authority is satisfied that the larger public interest warrants the disclosure of such information;

(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public

Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information".

The far-reaching implications of the above provision could be better understood by the decision of the Supreme Court in the case of Girish Ramchandra Deshpande vs. Central Information Commissioner ((2012) 8 SCR 1097). This is a case where a Special Leave Petition (SLP) was filed before the Supreme Court regarding the right to privacy with respect to information about public servants, in the context of Section 8(1)(j) of the RTI Act, which exempted the disclosure of certain information that might impinge on the right to privacy of the person about whom information is sought. The court answered the question whether the Central Information Commissioner, acting under the RTI Act was right in denying information regarding the third respondent's personal matters pertaining to his service career and also denying the details of his assets and liabilities, movable and immovable properties on the ground that the information sought for was qualified to be personal information as defined in clause (j) of Section 8(1) of the RTI Act. Observations of the court on the privacy rights are as follows:

"Para 12. The petitioner herein sought for copies of all memos, show cause notices and censure/punishment awarded to the third respondent from his employer and also details viz. movable and immovable properties and also the details of his investments, lending and borrowing from Banks and other financial institutions. Further, he has also sought for the details of gifts stated to have accepted by the third respondent, his family members and friends and relatives at the marriage of his son. The information mostly sought for finds a place in the income tax returns of the third respondent. The question that has come up for consideration is whether the above-mentioned information sought for qualifies to be "personal information" as defined in clause (j) of Section 8(1) of the RTI Act".

"Para 13 to 15- We are in agreement with the CIC and the courts below that the details called as above are qualified to be personal information as defined in clause (j) of Section 8(1) of the RTI Act. The performance of an employee/officer in an organization is primarily a matter between the employee and the employer and normally those aspects are governed by the service rules which fall under the expression "personal information", the disclosure of which has no relationship to any public activity or public interest. On the other hand, the disclosure of which would cause unwarranted invasion of privacy of that individual should denied. The petitioner in the instant case has not made a bona fide public interest in seeking information, the disclosure of such information would cause unwarranted invasion of privacy of the individual under Section 8(1)(j) of the RTI Act." And accordingly the court dismissed the subject SLP.

Courts on Privacy matters Post-Puttaswamy era

As narrated earlier, the right to information by a citizen has been treated as a fundamental right from the beginning whereas the personal information and the privacy matters have been considered as a fundamental right by the Apex court only after the judgement of the Puttaswamy judgment cited above [(2015) 8 S.C.C. 735]. Therefore, it is interesting to follow the decision of the Apex court, after the Puttaswamy decision, to find out the treatment of

privacy information under RTI act. The earlier orders and rulings may express different views for the pre-Puttaswamy period which are not relevant for our discussions. In view of the changed stand of the Hon'ble Supreme Court, the post-Puttaswamy cases are relevant to understand the treatment of personal information in the RTI realm. One such situation arose in the case of 'Central Public Information officer, Supreme Court of India v/s Subhash Chandra Agarwal', in Civil Appeal No. 10044 OF 2010 and the same is deliberated in the further part of this article. This landmark decision dated 13th November, 2019 determines the balance between the right to information guaranteed to all individuals with the principle of confidentiality and privacy. It provides equilibrium between the 'right to privacy', a newly recognized fundamental right, along with the disclosure of information by PAs, so as to move towards transparency in governmental services.

The facts of the case in brief are: - In 1997 at the Conference of Chief Justices, all the judges adopted a "Code of Conduct" which required them to disclose their assets in confidence to their Chief Justices. To see whether the judges are complying with the Code of Conduct, an RTI activist Subash Agarwal filed an RTI application seeking information from the Public Information Officer (PIO) of the Supreme Court. The PIO responded by saying that the information does not exist in the court registry. On appeal, the appellate authority directed the PIO to give name of the officer having the relevant information and to refer the application to the authority having the information by way of Section 6(3) of the Act. On remission the PIO rejected the application asking to file the application to respective High Courts. The applicant then approached the CIC. The CIC rejected the contentions of the Information Officer and directed him to provide the information. This led to a writ petition by the PIO in the Delhi High Court challenging the order of the CIC. A single bench judge decided that the order given by the CIC was correct. An appeal was filed against that decision given by the single judge bench, which is decided by the Apex court through this decision.

The bench of the Supreme Court deliberated the following questions of law, viz.,(1) Whether the disclosure of information to the public relating to the office of CJI and collegium system amounts to the interference of in the judicial independence?; (2) Whether section 8(1)(j) exempts the information sought for the public disclosure; (3) Whether the disclosure of information sought for, relating to judges would curtail or prevent the constitutional authorities from expressing their free and frank expression?

The Supreme Court vide its order dated 13/11/2019 dismissed the appeal and delivered the judgment in favour of respondent. The court upheld the Delhi High Court's judgment by directing the Central Public Information Officer, Supreme Court to furnish information regarding collegium decision-making, personal assets of judges, correspondence with CJI. It was further held that bar on disclosure of information cannot be imposed on the ground of free and frank expression of collegium member and the disclosure will be on case-to-case basis. During the deliberation in certain parts of the order, the Hon'ble judges have clarified the interplay of rights between RTI act and privacy rights. Important extracts are provided for appreciating the said subject matter.

Extract of the decision dated 13th November, 2019

"Para 40. The right to privacy though not expressly guaranteed in the Constitution of India is now recognized as a basic fundamental right vide decision of the Constitutional Bench in K.S. Puttaswamy and Another v. Union of India and Others holding that it is an intrinsic part of the right to life and liberty guaranteed under Article 21 of the Constitution and recognised under several international treaties, chief among them being Article 12 of the Universal Declaration of Human Rights, 1948 which states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. The judgment recognises that everyone has a right to the protection of laws against such interference or attack." The above observation provides the brief background of the privacy protection needs in the present-day society.

"Para 41. In K.S. Puttaswamy (supra) the main judgment (authored by D.Y. Chandrachud, J.) has referred to provisions of Section 8(1)(j) of the RTI Act to highlight that the right to privacy is entrenched with constitutional status in Part III of the Constitution, thus providing a touchstone on which validity of executive decisions can be assessed and validity of laws can be determined vide judicial review exercised by the courts. This observation highlights the status and importance of the right to privacy as a constitutional right…..It is observed that privacy involves a person's right to his physical body; right to informational privacy which deals with a person's mind; and the right to privacy of choice which protects an individual's autonomy over personal choices. While physical privacy enjoys constitutional recognition in Article 19(1)(d) and (e) read with Article 21, personal informational privacy is relatable to Article 21 and right to privacy of choice is enshrined in Articles 19(1)(a) to (c), 20(3), 21 and 25 of the Constitution. In the concurring opinion, there is a reference to 'The Right to Privacy' by Samuel Warren and Louis D. Brandeis on an individual's right to control the dissemination of personal information and that an individual has a right to limit access to such information/shield such information from unwarranted access. Knowledge about a person gives another power over that person, as personal data collected is capable of effecting representations in his decision making process and shaping behaviour which can have a stultifying effect on the expression of dissent which is the cornerstone of democracy. In the said concurring judgment, it has been further held that the right to protection of reputation from being unfairly harmed needs to be zealously guarded not only against falsehood but also against certain truths." The above observations provide the comparative legal analysis of Article 19 and Article 21 of the Indian Constitution.

"Para 42. Privacy, it is uniformly observed in K.S. Puttaswamy (supra), is essential for liberty and dignity. Therefore, individuals have the need to preserve an intrusion-free zone for their personality and family. This facilitates individual freedom. On the question of invasion of personal liberty, the main judgment has referred to a three-fold requirement in the form of – (i) legality, which postulates the existence of law (RTI Act in the present case); (ii) need, defined in terms of a legitimate State aim; and (iii) proportionality, which ensures a rational nexus between the objects and the means to be adopted to achieve them. The third requirement, we would observe, is achieved in the present case by Sections 8(1)(j) and 11 of the RTI Act and the RTI Act cannot be faulted on this ground. The RTI Act also defines the

legitimate aim, that is a public interest in the dissemination of information which can be confidential or private (or held in a fiduciary relationship) and larger public interest or public interest in disclosure outweighs the protection or any possible harm or injury to the interest of the third party."

" Para 53. While clause (j) exempts disclosure of two kinds of information that is "personal information" with no relation to public activity or interest and "information" that is exempt from disclosure to prevent unwarranted invasion of privacy, this Court has not underscored, as will be seen below, such distinctiveness and treated personal information to be exempt from disclosure if such disclosure invades on balance the privacy rights, thereby linking the former kind of information with the latter kind. This means that information, which if disclosed could lead to an unwarranted invasion of privacy rights, would mean personal information, that is, which is not having co-relation with public information."

"Para 59. Reading of the aforesaid judicial precedents, in our opinion, would indicate that personal records, including name, address, physical, mental and psychological status, marks obtained, grades and answer sheets, are all treated as personal information. Similarly, professional records, including qualification, performance, evaluation reports, ACRs, disciplinary proceedings, etc. are all personal information. Medical records, treatment, choice of medicine, list of hospitals and doctors visited, findings recorded, including that of the family members, information relating to assets, liabilities, income tax returns, details of investments, lending and borrowing, etc. are personal information. Such personal information is entitled to protection from unwarranted invasion of privacy and conditional access is available when stipulation of larger public interest is satisfied. This list is indicative and not exhaustive."

The above discussions clearly indicate that the listed information are to be treated as personal information eligible for protection both under RTI act and proposed privacy realm.

Third party information procedure under RTI act

Further, in instances where any confidential information that is pertaining to a third party are to be shared with the applicant, a mandatory procedure to seek the views of such third party before sharing the information to the applicant has been prescribed in the Act. As per section 11 of the RTI act, Where a CPIO or SPIO intends to disclose any information or record, or part thereof on a request, which relates to or has been supplied by a third party and has been treated as confidential by that third party, the Information Officer shall, within five days from the receipt of the request, give a written notice to such third party expressing intention to disclose the information or record, or part thereof, and invite the third party to make a submission in writing or orally, regarding whether the information should be disclosed. It further emphasizes that such submission of the third party shall be kept in view while taking a decision about disclosure of information. Once the PDP Act comes into force, this legal stipulation with regard to information pertaining to third party will be an extended protection to the Principal, who is treated as third party in RTI Act. This will be in addition to the procedure of obtaining the consent of the principal for collecting and storing of information his/her information by the Fiduciary, under PDP provisions. Thus, the privacy and confidential

matters are having reasonable restrictions in sharing it with the public under both laws as it is mandatory to seek the views of the data owner before deciding on parting of the data.

On this provision, the observations of the Apex Court in the above stated case are as follows:

"Para 61. We would clarify that Section 11 is not merely procedural but also a substantive provision which applies when the PIO intends to disclose information that relates to or has been supplied by a third party and has been treated as confidential by that third party. It requires the PIO to issue notice to the third party who may make submission in writing or orally, which submission has to be kept in view while taking a decision. Proviso to Section 11(1) applies in all cases except trade or commercial secrets protected by law. Pertinently, information including trade secrets, intellectual property rights, etc. are governed by clause (d) to sub-section (1) of Section 8 and Section 9 of the RTI Act. In all other cases where the information relates to or has been supplied by the third party and treated as confidential by that third party, disclosure in terms of the proviso may be allowed where the public interest in disclosure outweighs in importance any possible harm or injury to the interest of the third party."

Personal information with the Public Authority

It is a fact that all PAs are fiduciaries, but all fiduciaries are not PAs. As per the proposed PDP law, all PAs, including the Data Protection Authority (DPA) to be established for overseeing the initiation and implementation of the subject act, are treated as data fiduciary. The Section 49(3) of PDP Bill requires the DPA to be treated like any other fiduciary as far as the processing of the personal data is concerned. In view of the above legal position all PAs are mandated to adhere to the obligations of a fiduciary under the act. Accordingly the obtaining and processing of data by the PAs, in their fiduciary capacity or as an employer have to observe the modalities stipulated in the proposed law.

The PA may handle information of individuals broadly falling under two categories viz., of common public to whom they are rendering governmental services and the employees serving for the organisation in discharge of statutory functions of the organization. The personal information of both categories is subject to protection under RTI Act, as they are treated as third party under section 11. Their submissions shall be invited and considered before deciding the parting of the information to the applicant. The Supreme Court has held that such personal matters are to be considered case by case basis, and personal information should be denied to the applicant, if it involves threat to privacy rights of the individual. Under the proposed PDP Act, the individual to whom the personal data pertains to is treated as the owner /Principal and the PAs holding such personal information are treated as fiduciaries.

The PAs, in the role of fiduciaries for PDP Act, shall follow the prescribed procedure such as seeking the consent of the individual/principal after issuing due notice to the data owners for any of their activities. For obtaining the consent of an individual for collection or processing of personal data there is need of issue of a notice by the fiduciary, stating the reasons in clear, concise and easily comprehensible terms, to such person. Further such activities should be carried out, restricted to such purposes as consented, in a fair and reasonable manner, so as

to ensure the privacy of the individual. Such data have to be classified and protected as per this privacy law.

It is to be appreciated that such Principal /third party has the following rights under PDP Act: (a)the right to confirmation and access to the personal data with the fiduciary; (b) the right to seek correction of inaccurate, incomplete, or out-of-date personal data; (c) the right to have personal data transferred to any other data fiduciary in certain circumstances;(d)the right to restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn; (e) The right to receive the data from the fiduciary in a machine-readable format.

Further such a PA, treated as Fiduciary, while discharging the function as a fiduciary under PDP legal framework, is required to formulate a privacy by design policy that ensures (i) Managerial, organizational, business practices and technical systems are designed in a manner to anticipate, identify, and avoid harm to the data principal;(ii) The obligations of data fiduciaries;(iii) The technology used in the processing of personal data is in accordance with commercially accepted or certified standards;(iv) The legitimate interests of businesses including any innovation is achieved without compromising privacy interests;(v) The protection of privacy throughout processing from the point of collection to deletion of personal data;(vi) The processing of data is in a transparent manner; and (vii) The interest of the data principal is accounted for at every stage of processing of personal data. The data fiduciary should display the certified Privacy Policy on their websites and also submit its Policy to the Authority for certification in the prescribed manner.

Further the PAs, who are also fiduciaries, have to adhere to transparency and accountability measures under PDP like adoption of privacy by design by all fiduciary(Sec 22), security safeguards (Sec 24). In addition to maintenance of records (Sec 28), and conducting data impact assessments (Sec 27), any data breach in the organisation will have to be reported to concerned authorities (Sec 25). They further have to adopt audit policies (Sec 29) and provide grievance redressal measures (Sec 32) in respect of persons whose personal data they hold.

Personal information protection in coming privacy regime

As deliberated above, the RTI Act has sufficient safeguards in place to protect the breach of personal information by virtue of section 8(1) (J) exemptions read with Section 11 procedures in respect of third-party information. As all the personal information are protected under the proposed PDP bill, it is imperative for all PAs to register themselves as data fiduciaries and follow the norms stated above.

The PDP law proposes setting up of a Data Protection Authority (DPA) who may, (a) take steps to protect interests of individuals, (b) prevent misuse of personal data, and (c) ensure compliance with the Bill. Similarly, the PAs who hold the data, the CIC and SICs established under RTI act will have to consider the protection of personal data in the light of the new enactment and the stipulated harm audit before considering the section 11 procedure. From the above legal position, it can be concluded that there is no threat to protection of personal data in the combined PDP-RTI regime, as protection to privacy gets further strengthened. However as there are no definition provisions of certain common terms like ‘personal

information' "sensitive personal data" and 'Fiduciary' in the RTI Act, some ambiguities may set in. To avoid any such lapses, it is pertinent to borrow the definitions in the proposed PDP Bill to the RTI act through an amendment.

Recommendations

From the factual and the legal position deliberated above it is evident that there is no conflicting situation between the objectives of RTI act with reference to provisions of the PDP provisions. Both the enactments are complementing and supportive to each other and enable protection of the fundamental rights of the citizen which is essential for a peaceful living. As noted above, certain amendments are suggested in the RTI Act, so that there is no scope for ambiguity in the entire legal framework. The terms like 'personal information/data '(Sec. 3(28) of PDPB) "sensitive personal data" (Sec. 3(36) of PDPB) and 'Fiduciary' (Sec.3(13) of PDPB) could be borrowed through an amendment to RTI Act, to have the meaning similar to PDP act, so that there is holistic approach could be achieved in protection of the privacy rights of the citizens.

DATA TRUST SCORE – THOUGHTS ON LEGAL FRAMEWORK

M.G.Kodandaram

Consequences of Data Trust Score

The much awaited Personal Data Protection Bill, 2019 ('bill' hereinafter for brevity) is awaiting the scrutiny of the joint parliamentary committee, who are in final leg of their consultation and finalization process. The sub-section (5) of Section 29 of the bill relating to Audit of policies and conduct of processing as a measure of transparency and accountability to be adopted by a data fiduciary specifically mandates, "A data auditor may assign a rating in the form of a data trust score (hereinafter 'DTS') to the data fiduciary pursuant to a data audit conducted under this section". The bill authorises the auditor, conducting the compliance verification of a fiduciary, to measure the trust worthiness of such an entity by awarding a score to be prescribed through regulations by the Authority, as an indicator1. The scores so awarded should be published by the fiduciary in the notice issued to the principal2 and in the web maintained by the entity in the manner prescribed by the Authority3. These scores should also be announced by the Authority4 in their public domains. This stipulation makes the DTS process, a more sensitive proposition as such scores will have huge ramification on the goodwill, investment and the service decisions in respect of such fiduciaries in the competing market place. Therefore it is of utmost importance to devise a justifiable scoring comprehensive pattern and configuration so that there is a fair approach in place for assigning the trust score.

As we are aware that the privacy of an individual is a very subjective issue and for this purpose, the levels of protection in place at the disposal of a fiduciary are not easily measurable in arithmetical terms. It is a well known principle that only those that are measurable could be gauged and monitored. Therefore one should explore for a system which could indirectly assist in assigning such a score with least scope for ambiguity or bias on the part of the compliance auditor. There is no availability of similar tool employed for this purpose elsewhere as no such prescriptions exist in other privacy laws in force around the globe. This is a unique positive approach by the Indian authors of law to stipulate such a mechanism for the first time. In view of the above facts, the quest for a fair and justifiable method for computation of the DTS becomes all the more challenging. An attempt is made here to suggest the ways that could be adopted for this purpose.

The best way to initiate the search for a fair solution, the author feels, is to examine the related provisions in the bill to find out the intentions, objectives and methods embedded in the proposed statute. The solutions should be within the substantial law and should not to transgress the stated perimeters. If any essential factors are missing, the same should be recommended to be part of the law in the making. With these thoughts in the background, the essential legal framework applicable to DTS, as available in the proposed law, or required to be incorporated in the law, if in case of such need arises, are deliberated in the further part of this article.

Impact of proposed law on stake holders

The proposed bill is going to impact every individual's privacy in the present cyber society as all the services and activities, by the Government or by business and non-business entities, are being built around the digital technology as an essential component. In all walks of life, every citizen (you may call them as 'netizen') encounters the privacy issues in all types of communication with others. Therefore one can assume that the entire population residing in the country may have to be treated as 'Principals' of some fiduciary or processors at one stage or time. It could be a visit to a commercial centre or consultations with a doctor or an academy for education or any activity of assorted instances which cannot be narrated at length, where the Principal's personal data are being collected and processed. Almost all the entities involved in dealing with individual's personal matters, automatically qualify themselves as data fiduciary, unless they are either kept outside the applicability of the provisions or specifically exempted under the provisions. Now it is left to the guesstimate of the readers to assess the volumes of data and impact on managing such data. The bill places full responsibility on the data fiduciary to protect the privacy rights of the principal and any breach of this assurance make them liable for penal actions. Punitive measures for breaches and violations by the fiduciary could be initiated by the principal or the Authority, and adjudicated by the Authority and courts. In view of the above legal position, one can conclude that implementation of privacy laws is going to be a change of a massive scale and proportion. Therefore all the stake holders need to prepare sufficiently in advance, both in terms of technology and legal procedures, to absorb and follow the changes.

Legal provisions relating to DTS

The Section 29(6) of the bill declares that, 'the Authority shall, by regulations, specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (2)'. The subsection (2) specifies the criteria for assigning a data trust score which are discussed in the later part. From the stated stipulations the conclusions that could be drawn are, (i) evaluating the score is the responsibility of the privacy data auditor appointed by the Authority; (ii) such compliance audit in respect of a data fiduciary should cover the examinations and observation of the auditor under Sections 7,22,23,24 and 25 of the bill; (iii) the process for scoring are not left to the wisdom of the auditors, but are to be regulated by the Authority. Therefore there is legal necessity to notify the DTS regulations before going for implementation of the DTS provision.

The various powers of the Authority to make regulations are listed in section 94 of the bill. The Authority may, by notification5, make regulations consistent with this Act and the rules made thereunder to carry out the provisions of this Act. The section 94 (2) lists out the matters that could be regulated, and among them the following are relevant for our discussions. "(l) the other factors to be taken into consideration under clause (g) of sub-section (2); the form and procedure for conducting audits under sub-section (3); the manner of registration of auditors under sub-section (4); criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary under sub-section (6) of section 29;

(g) the manner for submission of privacy by design policy under sub-section (2) of section 22."

It must be noted that it is regulations to be made and not the rules, meaning that such matters (auditors, privacy by design and DTS) should be directly controlled and monitored by the Authority. The Authority may, by notification, make regulations consistent with this Act and rules to implement the DTS provisions.

Evaluation of fiduciary by Data Auditor

As per Section 29 of the bill, a significant data fiduciary shall get its policies and the conduct of its processing of personal data, audited annually by an independent data auditor. Further the Authority6 have powers vested with them to direct any data fiduciary to get an audit carried out by an appointed data auditor, if they are of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal. Therefore we can deduce that it is mandatory for all significant fiduciary to get audited annually and for others, it is the on the performance of fiduciary as observed by the Authority. However such proposals should normally be through written directions that could be part of the regulation.

The parameters to be used by a data auditor to evaluate the compliance of a data fiduciary includes, "(a) clarity and effectiveness of notices under section 7; (b) effectiveness of measures adopted under section 22; (c) transparency in relation to processing activities under section 23; (d) security safeguards adopted pursuant to section 24; (e) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25; (f) timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and (g) any other matter as may be specified by regulations." As this is an inclusive provision similar parameters could be added in the form of regulations, within the principal framework of the bill. It is the responsibility of the Authority to, not only notify the forms and procedures for conducting audits but also appoint persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, as data auditors under the Act. This provision leads to formation of a new stream of auditors specialised in privacy law and appropriate technology, after due entrance examination and personality tests that could be formulated under the regulations. This is one of the most critical aspects in effective implementation of privacy laws as such auditors are to exercise the responsibilities of compliance audit, followed by assigning DT score of the registered fiduciaries. Now we shall examine each of the above prescribed factors to explore the ways to compute the principles in the proposed DTS.

Issue of notice to principal

We shall examine each of the factors prescribed in Section 29 of the bill to explore the ways to compute the principles in the proposed a fair and justifiable Data Trust Score. Every data fiduciary shall issue a notice to the data principal before the collection or processing of personal data and the contents contained in such form is one of the factors to be considered

to evaluate the trust score. Some factors indicated in section 7(1) of the bill, among others, include the following which are relevant for the present discussions.

"(k) the procedure for grievance redressal under section 32;

(l) the existence of a right to file complaints to the Authority;

(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and

(n) any other information as may be specified by the regulations".

From the above it is to be noted that (i) having a grievance redressal as prescribed in section 32; (ii) principal's right to file complaints to Authority and (iii) intimating the data trust score assigned under section 29(5) to the data principal, are the important factors to be considered by the auditor to evaluate the trust score of a fiduciary. To enable higher rating of DTS, it is important for the fiduciary to have a dynamic grievance redressal mechanism in place. At the same time it is the responsibility of the Authority to provide a tool to lodge complaints by the principal and to suitably redress them.

Redressal of grievances of principal

As mandated under section 32 of the bill, every data fiduciary should provide an effective mechanism for redressal of grievances of the data principals. The facility for lodging a complaint by the principal for any contravention of the provisions that has caused or is likely to cause harm to her/him is an essential responsibility of the fiduciary. Such a facility must be managed by the data protection officer or designated officer of the entity. Complaints received have to be resolved by the data fiduciary in an expeditious manner, within 30 days of receipt of the complaint. If such complaints are rejected or not resolved within the time frame, or if the principal is not satisfied with the manner of disposal, the data principal may file a complaint with the Authority. Therefore the Authority is expected to host a separate facility for receiving complaints from principal against such unattended grievances.

As the volumes of transactions are expected to be high, it is expected that these services to the principal could be built by the fiduciary and the Authority together in digital mode. For this development of a central digital facility by the Authority in association with the entities are preferred, as it eases the complaint filing mechanism to the principal, and further monitoring, disposal as well as recording of the entire process could be automated. The quantum of transactions and timelines followed in redressal process could be used as a realistic data source to measure the trust score in respect of each of the fiduciary at one place.

However it is interesting to note that there is no mechanism inbuilt in the bill to obtain feedbacks of the principal.

Privacy by design policy

The second factor to be considered for awarding the score by the auditor is the effectiveness of measures adopted under 'Privacy by design' policy as mandated under section 22 of the bill. The Bill mandates that a data fiduciary is required to formulate policy that (a) ensures

Managerial, organizational, business practices and technical systems designed in a manner to anticipate, identify, and avoid harm to the data principal, (b) meets the listed obligations towards protection of personal data, (c) uses the technology in accordance with commercially accepted or certified standards, (d) protects the legitimate interests of businesses including any innovation is achieved without compromising privacy,(e) protection of privacy throughout the processing, from the point of collection to deletion of personal data, (f) processing of data in a transparent manner and (g) interest of the data principal at every stage of processing of personal data. The data fiduciaries should submit the policy so prepared to the Authority for certification within the prescribed period. The Authority after due verifications of the information and compliance having been provided as prescribed under Section 22(1), shall certify the same. The said information need to be published in the official websites of the Authority and of the fiduciary concerned. This entire process could be built on a digital platform and the emerging data could be used to gauge the trust score.

Transparency and security measures

Transparency in relation to processing activities under Section 23 is the third factor that needs to be considered in awarding the data score. The fiduciary should make available, in prescribed form and manner, the information namely, "(a) the manner and categories of personal data generally collected; (b) the purposes for processing the personal data; (c) any probable risk of significant harm in such processes; (d) the facilities available for the data principal to exercise rights regarding access, correction, erasure, portability and such other rights vested under law; (e) the right of data principal to file complaint against the data fiduciary to the Authority; (f) where applicable, any rating in the form of a data trust score accorded to the data fiduciary under section 29(5); (g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and (h) any other information as may be specified by regulations."

The fourth factor that needs to be considered is the security safeguards adopted by such entity pursuant to section 24 of the bill. Every data fiduciary and the data processor shall implement and review periodically the necessary security safeguards, such as, "(a) the use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data". These could be verified by the auditor who can list out the gaps to arrive at the data score relating to the fiduciary. Similarly the instances of personal data breach and timely response of the data fiduciary, including the promptness of notice to the Authority under section 25, timely implementation of processes and effective adherence to obligations under section 28(3), being the fifth and sixth factors, that could be verified by the auditor to draw fair conclusions.

In this concluding part we shall deliberate on the fair means to use of the mandated principles within the scope of the objectives and the proposed legal framework, to arrive at the possible data score methodology. The author is not inclined to propose a definitive scoring pattern as the bill in hand is still a legislation in the making and more changes are expected before it becomes the law of the land. Once the legislation gets the nod of both the houses, carrying

out such an exercise will be more realistic and useful. Therefore the discussions are limited to the components that should be part of the DTS system.

Objectives of the bill

The Preamble part of the bill declares the purpose of the legislation as, "to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data". It further vouches (i) to protect the rights of individuals whose personal data are processed, (ii) to create a framework for organisational and technical measures in processing of data, (iii) laying down norms for accountability of entities processing personal data,(iv) remedies for unauthorised and harmful processing, and (v) to establish a Data Protection Authority of India for the said purposes. The honourable Supreme Court in the case of Justice K.S. Puttaswamy7 v/s Union of India has held that right to privacy is a fundamental right and therefore it is necessary to protect the personal data as an essential facet of informational privacy. At the same time it is necessary to create a collective culture that fosters a free and fair digital economy, ensuring empowerment, progress and innovation through digital governance. No doubt that the data is the lifeblood of any digital business, but on its abuse, the ultimate losers are the consumers, who may receive an irreversible shock on their private life.

Obligations of the fiduciary

The privacy rights of an individual has to be accomplished for which the data fiduciaries are expected to follow certain obligations stipulated under section 4 to section 11 of the bill. The Bill allows the processing of data by Fiduciaries only after the due consent is obtained from the individual / Principal. For obtaining the consent of a Principal for collection or processing of personal data there is need of issue of a notice by the fiduciary to such person, stating the reasons in clear, concise and easily comprehensible terms. The procedure for issue of notice to the principal, at the time of collection of data8, for obtaining the consent is elaborate and due care to be taken to devise digital tools for meeting the requirements. In the notice the Principal should be informed about the purpose, nature and categories data being collected. The identity and contact details of the data Fiduciary and the contact details of the data protection officer are also to be informed to the Principal. Such Principal should be informed of the procedure to withdraw his consent in the mandated way. Further a personal data can be processed only for specific, clear and lawful purposes. The Data Fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it was processed and shall delete the personal data at the end of processing. The personal data may be retained for a longer period only after the data fiduciary gets necessary consent from the Data Principal. During the compliance audit, it is for the data auditor to comment on each one of these parameters followed by the fiduciary, before proceeding for the quantification of DTS score. The measure so made should indicate the trust factor of the fiduciary in handling the personal data of the principals.

It is pertinent to mention here that the relationship between the principal and fiduciary enshrined in the bill are of special and unique nature. Here the fiduciary should extend a breach-proof mechanism to the personal data owner / principal which are equivalent to safeguarding the fundamental rights of the principal. Therefore the measure applied to score the 'trust-worthiness' needs to be rational and realistic. Efforts should be made to measure directly or indirectly all the stipulated obligations, compliances and functions of the fiduciary, and by using digital tools, wherever possible to meet the meet the requirement of law.

Voice of principal needs recognition

From the above deliberations we find that there are compliances mechanisms and complaint mechanism in place but the crucial element of feedback mechanism is missing in the entire framework under consideration. As stated in the earlier part, the major stake holder or the beneficiary in this entire bill is the principal, but her/his observations about the services rendered by the fiduciary are not provided due place in scoring the credentials of the fiduciary. Further any personal data breach that takes place at the fiduciary's location, through the dark nets may land in the hands of the cyber criminals, who could exploit the data to cause injury to the principal. The safeguards taken by the fiduciary to eliminate personal data breaches protects the principal from being a victim of cyber crime. The satisfaction of the principal about the protection layer provided by the service providing fiduciary is an important element in measurement of trust score. The DTS is supposed to express the trust of the principal as to the level of protection the fiduciary has extended. Therefore the principal's feedback about the satisfaction in the services provided by the fiduciary will be one of the best indicators of mutual trust, the author feels.

Finding fault or gap in services should not be based on the mere observations of the auditor or on sheer outcomes of the complaint mechanism in place. The principal's voice should be heard which deserves a place in formulating the score for the fiduciary. Therefore a feedback system should be legislated wherein the fiduciary should be asked to obtain responses from their principal whenever they provide them with any service. This will also adds value to the review mechanism of the fiduciary.

As per the above deliberations it is clear that there is no provision made in the law for a principal to offer the feedback about the services extended by a fiduciary. This needs to be used as a positive aspect to draw the trust scores, the author observes. A suitable section could be inserted prescribing an effective feedback mechanism and using them to determine the scoring of the data trust.

Authority to be well equipped

Further in a Democratic society like Bharat, to take up the huge responsibility of implementation of this law and the disproportionate issues that could emerge, the Authority concerned should be well equipped in terms of skilful techno-legal manpower along with robust digital platform to be used as e-governance vehicle. As per section 49 of the bill, "It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection" which a huge responsibility to be discharged. Further the

responsibilities Authority include, (i) taking prompt and appropriate action in response to personal data breach (ii) maintaining a database and the data trust score on the web, (iii) classification of data fiduciaries, (iv) monitoring technological developments and commercial practices that may affect protection of personal data,(v) receiving and inquiring complaints, (vi) selection of auditors,(vii) prescribing the design by policy and DTS measures, together with registration and regulations of various provisions relating to safeguard the interest of the principals are going to be matters of great concern.

As the task involved is around safeguarding the fundamental rights of a citizen, it becomes all the more important as the Supreme Court and high courts could be directly approached for reliefs. Added to this the technological advancements are on an accelerated mode, so also the information exchanges and communications as well as the cyber crimes. Unless the officials are proportionately equipped with techno-legal skills, the implementation of law may leave huge scar in governing of citizens. The Authority must select officials with requisite technical and legal qualifications only. Such executives are to be suitable trained which is going to be the most critical element for the successful implementation of this new regime.

The section 49(3) requires the Authority to be treated like any other fiduciary as far as the processing of the personal data is concerned. It expressly mandates that, “it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that is treated as confidential by the data fiduciary or data processor, it shall not disclose such information unless required under any law to do so, or where it is required to carry out its function under this section”. This is a crucial aspect of the bill that deserves special attention. Further all the central government departments are following the standards prescribed under Service Quality Management System as per IS 15700- SEVOTTAM, which should be made applicable the Authority.

Conclusions

The computation of DTS by the auditor to be fair and justifiable may consist of the following major components:

(1) Outputs from the measurable components like (a) dynamic grievance redressal mechanism; (b) online periodical compliance by fiduciary; (c) reported breaches and remedial action taken along with time frame. etc.,

(2) Outputs from the verification report drawn by the data auditor on subjective issues such as obligations met by the fiduciary, appreciations and deficiencies noticed during the audit etc.,. and

(3) Feedbacks from the principal about the quality of the services provided as against the mandated obligations and the trust she/he could recommend.

(4) The Observations by the executives who are implementing these provisions.

The suggested weightage to obtain the consolidated DTS score form the above four components could be, for first three components, 30% each and 10% for the last. The author welcomes any additional suggestions and ways to measure the trust score so that it becomes the forerunner in the cyber society and the best practices to ensure privacy of the individual.

1 sec. 22(5), PDP bill

2 sec. 7(1) (m), ibid

3 sec. 23(1) (f), ibid

4 sec. 49(2) (c), ibid

5Sec. 29 (7), ibid

6 Sec. 29(7), ibid

7 (2015) 8 S.C.C. 735 (India)

8 Sec.7, PDP bill

Q & A

Here are a few questions that FDPPI has come across recently and some view points from FDPPI team:

Q 1: As per the current legal provisions, who is competent person to provide 'consent' for PII processing of an adult who is mentally challenged/lunatic/person in vegetative physical and mental status.

A: Consent is a contract and the person in a mentally incapacitated state has to be represented by the guardian. Guardian can be a natural guardian or a Court appointed guardian. In case of a natural guardian, it is preferable to obtain a medical certificate about the incapacity.

Q2: What do consider your biggest risk when it comes to data?

a) Hackers

b) Sloppy Third Parties

C) Internal Bad Actors

d) Outdated Policies and Procedures

A: Since penalties for non compliance of Data Protection laws can arise from one or multiple reasons, it is not necessary to rate the different types of risks. All risks are equally important and equally damaging.

Q3: The PDP Bill fends only for economic aspects of Privacy but does not provide for any rights against the state despite it being a fundamental right. How can Government be incentivised to incorporate rights against the State?

A: This is not a correct perception. PDPB2019 includes Government bodies as data fiduciaries. There are however some exemptions under reasonable exceptions provided for fundamental rights under Article 19(2) of the constitution.

Further the heads of departments are liable like CEOs of companies for vicarious liability subject to due diligence protection.

Q 4: Do You foresee any conflict between RTI act and PDP Bill?

A: It is natural. However Right to Information is also a right that is important for individuals in a democracy. It is also required for security reasons of the individual. PDPB 2019 expects that the person responsible for release of information under RTI will conduct a “Harm Audit” and decide if the information may be released.

Q 5: Since the Court hearings are now online and open hearing is the part of the rule of law, how do we balance the right to privacy of the parties against this? Is there a need for specific law to deal with the privacy of judicial data?

A: Privacy is not an absolute Right. It has to survive with other various rights. Citizen has a right to know if our Judiciary which is the key pillar of our democracy is fair and is functioning properly. Online hearing per-se may allow only the litigants and the counsels attend and hence there is no privacy issue..

The move to hold some sessions online with public access is different. It is like a public hearing as compared to an "In-camera" hearing. This is a great move which has to be appreciated. It is educative for the public to know how the Courts are functioning. It will also place the counsels and Judges under public scrutiny. It will perhaps reduce arbitrariness of the Courts and even corruption. Hence it is a move to be appreciated and welcome.