

# DPDP Act - Inputs for consideration

## Comments on Sections of the DPDP Act

Since Nov 2022, when Chat GPT was released, personal data has assumed far greater importance both for technology companies and for the individual. The greatest drawback for the individual consumer is her ignorance of the significance of impact of the training data used by AI/ML companies on her. This ignorance leads to the consumer embracing the benefits (productivity improvement) unwittingly without giving a thought as to how the parting with the data might adversely affect her. The exponential growth trajectory and the massive funding driving the growth of the AI industry makes it hard for all actors including Governments to keep pace with AI and protect consumers.

1. Section 2 (t) definition of personal data is not broad or detailed enough for a data law in the AI/ML age. AI/ML uses personal data as the input for AI training. Personal data needs to be categorized according to its function and resulting levels of protection required to be implemented by AI/ML and other programs. Only after this is done can the appropriate levels of security controls be applied in the law. Some personal data (PD) categories can be used by the data fiduciary for identification purposes and are at the lowest level of security of PD. Other PD parts like medical data are at a higher level of security and need to be addressed appropriately in the law. Even higher for security purposes are the psychometric profiles of individuals which may be exposed for specific approved purposes only.

Another example of PD classification is Personal Profile data (PPD)<sup>1</sup> or Personal Real-Time data (PTRD)<sup>1</sup>. Personality traits, cognitive abilities, emotional intelligence, behavioural preferences, values and motivations, attitudes, beliefs and communication styles are part and parcel of our personality profile. Human Uniqueness Data (HUD) is explained in ‘Keep your personal data secure from AI’<sup>4</sup>. The capture of these aspects and AI simulation/emulation/misuse can result in undermining our uniqueness as individuals. The PD law should prevent AI from undermining or misuse of human individualities.

With the advent of personal AI agents, active listening and other techniques, AI is now being trained on all these PD categories which require high level of security. Therefore, the definition of personal data needs to be strengthened and broadened to provide hierarchical levels of security for PD.

2. Section 4(1) a) Active listening<sup>2</sup> is already taking place on mobile phones, yet it is carried out without any consent of the consumer or even without acknowledgement of the activity by the technology company carrying out active listening. There is no way to check whether active listening is taking place unless we examine the code and database both on the personal device and on the server of the technology company. It is extremely difficult to achieve this verification and hence it is not a practical approach.

The same is true in the case of the “Journal” app provided by Apple in iPhones. By using both these methods technology companies treat the human being as the scapegoat for commercial profit in an unethical and devious manner. Unfortunately, employees are not able to call out these unethical practices since their jobs are at stake. The Government should

recognise this important constraint which is being exploited by companies. This is an important area which the PD law should protect.

Whereas, if the storage and processing of personal data is done only on the handset/ tablet/laptop as explained in my paper<sup>3</sup> it becomes a foolproof solution.

3. Section 8 (4) and (5) of the DPDP Act needs to be studied in greater depth. In the case of one Data Fiduciary passing on customer data to another data processor there is a linked chain effect. Meta in its contracts washes its hands off how its vendors handle of personal data. Meta T&C state “By using AIs, you are instructing us to share your information with third parties when it may provide you with more relevant or useful responses. Those third parties will use any information that we share – which may include personal information about you or others – in accordance with those third parties’ privacy policies.” Ideally Meta should say that it has signed contracts with all vendors to ensure personal data protection at the same level as itself unless other functional criterion are involved. These functional criteria should also be listed and clarified in the T&C agreement.
4. Section 9 does not cover the prevention of behavioural monitoring of normal adult consumers. The functional aspects of behavioural and activity monitoring could extend well beyond marketing purposes and venture into psychometric profile data capture which requires higher levels of PD security as explained above in Section 2(t) above. These aspects need to be addressed in the DPDP to protect consumers from parting with their data unwittingly.
5. Section 10(2) b) independent audit of significant Data fiduciary. How can this be achieved in a fool-proof manner when watermarking technology is in the hands of the technology companies? In the case of all other data (other than personal data), the wordings of this section should suffice. It is my view that in the case of personal data, it is too dangerous to permit its possession by data fiduciaries as long as the commercial temptation to profit and business growth exists. Moreover, it is the fundamental right of the individual to possess and protect his own data for storage and processing as per his choice.

## Other comments and areas to be addressed

### Personal Agents

Personal agents have not been mentioned in the DPDP Act. Yet it is through AI agents that tech companies will collect most personal data for training. Since personal agents impact the most sensitive parts of PD, they need to be addressed appropriately in the law. The capturing of a person’s intentions, psychological profiles (which consist of information listed in para 1 above) is extremely sensitive information. The capture of PD by personal AI agents and its use should be regulated by law.

### Simulating the Human Mind

The simulation of the human mind is the Critical Technical Milestone (CTM) <sup>1</sup>. At present, AI data laws should prevent AI from attempting to simulate the human mind in the quest for Artificial General Intelligence (AGI) since we are not yet aware of the implications of runaway growth of AI/ML. As things get clearer over time with AI technology progress this law may be revisited.

## Protecting Constitutional Guarantees

1. The most important argument is that as per the Constitution of India the right to property cannot be denied to any person. Since the person (consumer) owns his own personal data, it is his property, and he should be able to safeguard his property in the best possible manner. The best way to do this is to limit the personal data to storage and processing only on the personal device and make it unlawful for companies to take it away from the device. My attached paper on 'A practical solution for the conundrum of AI and personal data' explains how this can be done.
2. All AI functionalities regarding personal data should be switched off in factory settings when the personal device is initially purchased or resold. After purchasing the device, the owner should have the facility to switch on only those chosen AI functions which he prefers to use. This arrangement serves two purposes viz. it prevents the vendor company from processing/handling the data except on the device and ensures the owner has herself enabled the AI functionality on the device and therefore taken responsibility for that AI function to run on her device.

### References:

1. Why and how to control AI – Rajagopal Tampi [Why and how to control AI - aipathfinder.org - Pathfinder for Artificial Intelligence](https://aipathfinder.org/Pathfinder-for-Artificial-Intelligence)
2. <https://www.msn.com/en-in/money/news/is-your-phone-listening-to-your-conversations-yes-and-there-is-finally-proof-story-in-5-points/ar-AA1q7qyv?ocid=msedgdhp&pc=LCTS&cvid=84bea0f924d847f0a4d28e3d139dd94a&ei=20>
3. [A practical solution for the conundrum of AI and personal data - aipathfinder.org - Pathfinder for Artificial Intelligence](https://aipathfinder.org/Pathfinder-for-Artificial-Intelligence)
4. [Keep your personal data secure from AI - aipathfinder.org - Pathfinder for Artificial Intelligence](https://aipathfinder.org/Pathfinder-for-Artificial-Intelligence)

Disclaimer: The opinions expressed in this paper are personal opinions and futuristic thoughts of the author in his genuine quest for designing AI systems in a Human-Centric and Explainable manner. No comment or opinion expressed in this document is made with any intent to discredit, malign, cause damage, loss to or criticize or in any other way disadvantage any person, company, government or global and regional agencies.