Na.Vijayashankar (Naavi)
37, Ujvala, 20th Main, BSK First Stage
Bengaluru, 560050
Phone: 9343554943
E-mail: naavi@naavi.org : Web:www.naavi.org

Concerns on DPDPB 2023

Medianama	Naavi.org
The government's broad powers to exempt itself, demand information from companies, and retain data for an unlimited period can result in mass surveillance: The DPDP Bill allows the government to issue a notification to exempt any of its agencies from the Bill on grounds like the **security of the State, maintenance of public order.** etc. In other words, any exempted agency of the government can collect and process the personal data of citizens without following any of the safeguards prescribed in the DPDP Bill and for any purpose they want. Additionally, Section 36 allows the government to demand personal data from private companies "for purposes of this Act," which is not a phrase that is elaborated. Both these provisions, combined with the fact that the government can retain personal data for an unlimited period regardless of whether the purpose for which it was collected has been served, means that the government has a carte blanche to carry out mass surveillance. Furthermore, there is an automatic exemption for processing personal data for the prevention, investigation, etc., of crime, without the need for the government to issue any notification.	The reasonable restrictions to the Right to Privacy is provided under Article 19(2) and accordingly processing of data for purposes such as security of state has been exempted. The interpretation of Section 36 is mischievous and incorrect. There is no such implication in the Bill that the Government may demand personal information under this section. This kind of interpretation indicates that certain persons are thinking of denying even legitimate information to the Government from the Data Fiduciaries and if this is so, they are only interested to carry on an illegal activity under the guise of Privacy. Government has a duty to provide security to its citizens and hence certain powers to retain information even of personal nature belonging to the citizens is the legitimate requirement of Governance. It is strange that even for processing information for law enforcement there is a demand for a notice. This essentially means that all criminals should be given prior notice that their information is being tracked. The objection is therefore completely unacceptable.
2. Free pass for scraping of publicly shared personal data: Clause 3(c)(ii) of the Bill states it shall not apply to personal data that is made publicly available by the user. As an example, the Bill illustrated that if an individual, while blogging her views, has publicly made available her personal data on social media, then processing of that data won't come under the purview of the data protection law. This allows companies to process publicly available personal data without any consent or without adhering to any other provisions of the Bill. For example, AI services like OpenAI's ChatGPT and Google Bard will be able to scrape publicly available personal data from the internet to train their models.	If personal data is made publicly available by the Data Principal there is no reason why there should be any objection. We may note that the law says" Made publicly available" and not "Is publicly available". Hence consent is ingrained in this provision. As regards 3(c)b(ii)(B), the consent is not required as the information is made public under a legal obligation. If we recognize the difference between "Publicly Available" and "Publicly made available", then the objection becomes unsustainable.

Na.Vijayashankar (Naavi)
37, Ujvala, 20th Main, BSK First Stage
Bengaluru, 560050
Phone: 9343554943
E-mail: naavi@naavi.org : Web:www.naavi.org

This also raises possibilities of facial recognition tools using publicly available profile photos to train their systems.	
3. Definition of child as someone under the age of 18 creates access issues for children and a compliance burden for companies: The DPDP Bill has additional obligations for companies processing data of children, defined as anyone under the age of 18. Importantly, it requires such companies to get "verifiable consent" from parents before processing children's data. This not only takes away agency from teenagers by restricting their ability to access websites without parental consent but also puts companies in a tough spot as they will have to carry out some form of age verification (which itself would require collecting personal data such as government-issued IDs) of all their users to ensure that they are not collecting personal data of any children without parental consent. The Bill allows for some companies to be exempt or have a lower age threshold if they process children's data in a way that is "verifiably safe." But it is not clear what fits this criteria and it creates two different standards for companies processing children's data. A seventeen-year old and an eight-year old should not be treated the same and a graded approach should be adopted by the Bill.	This objection clashes with the necessity of the society to "Protect Children" from certain dangers. All over the world similar legal measures of restricting access to certain information based on age is used. The issue of age verification and obtaining consent from guardian is also a global phenomenon which does not have an easy solution. Whether the actual age at which restrictions be removed should be 18 or less is an academic debate. If Consent is a form of contract, then contract law has to be respected and 18 year cut off also has to be respected. Since DPDPB 2023 considers a child as a joint data principal with the guardian, the consent of the joint data principal will be required. Use of "Digital Age" concept and introducing measures to switch parental consent to individual's consent during a period surrounding the attaining of 18 years has been discussed by Naavi.org earlier and can be considered during the notification. The "burden" on data fiduciary for obtaining verifiable consent is a reality and has to be met by data fiduciaries who are providing services to children.
4. The government's power to block content goes beyond the already controversial Section 69A of the IT Act: Under Section 37, the government can block access to websites or content on advice from the Data Protection Board in case of repeated offences by the entity or in the "interests of the general public." This broad phrasing goes beyond the already controversial powers of the government to block content under section 69A of the Information Technology Act of 2000. Additionally, the powers of a Data Protection Board to advice on blocking "content" is problematic given that the Board is entrusted with issues related to data protection and "content" is a broader ambit that other regulations such as the IT Act already deal with.	Section 37 only empowers the Data protection Board which otherwise has quasi judicial powers to advise the Government to initiate action for blocking access when required. This is only a supplement to Section 69A and actually reduces the power under Section 69A making it mandatory for the authority under 69A to require a written request from the DPB for blocking. The objection is therefore is invalid ab-initio.

Na.Vijayashankar (Naavi)
37, Ujvala, 20th Main, BSK First Stage
Bengaluru, 560050
Phone: 9343554943
E-mail: naavi@naavi.org : Web:www.naavi.org

5. The "as may be prescribed" Bill: The phrase "as may be prescribed" appears at least 26 times in the 20-page bill leaving a lot to delegated legislation. This allows the government to notify rules later on to clarify these provisions. Such rules don't go through the same parliamentary rigour as the bill itself, because of which these rules can be overbroad and go beyond the scope of the parent legislation, as is being argued about the IT Rules of 2021, which was issued under the IT Act of 2000.	It is not feasible to hard code all requirements on regulation of a dynamic domain such as "Data Protection" and hence resorting to notifications is unavoidable. GDPR regulators actually created WP29 system now managed by EDPB for issuing such regulations, notifications on an ongoing basis. It has been a practice for these activists to take every rule and notification directly to Supreme Court and the Supreme Court obligingly uses its powers to scrap many such notices as we have seen in the context of ITA 2000 notifications or UIDAI related notifications. In case of UIDAI and IRCTC even routine tender documents have been referred to Supreme Court alleging infringement of fundamental rights and the Supreme Court is most obliging to consider such complaints. The objection is therefore without substance.
6. Weakens the RTI Act by giving the government more reasons to deny information: The DPDP Bill amends the RTI Act of 2005 to state that the government is not obliged to disclose information that relates to personal information. Earlier this could be overridden in case of larger public interest. By making this amendment, the Bill weakens the RTI Act as the government has one more broad ground to deny information requested. "A new era of corruption will be introduced as personal data like assets and liabilities, education qualifications of corrupt officials, won't be sought under RTI Act," MP Adhir Chowdhury pointed out in the parliament.	Right to Information and Privacy are opposing principals and conflicts cannot be avoided. At the same time RTI should not be mis- used for extracting personal information. Such cases need judicial intervention and the aggrieved RTI activist need to get Judicial order to extract personal information which is feasible. The objection is therefore speculative.
7. No consent is required for sharing data with others: When obtaining consent, a company does not have to disclose who all the data will be shared with and for what purposes.	The pervious version of notice under DPA 2021 and DPDPB 2022 was detailed and was very cumbersome. This has now been simplified. Even under GDPR, such information is required to recognize only "Types of processors" to whom data is shared and not the names of the processors and sub contractors. These are business sensitive information that cannot be shared without damage to the business of the organization.
8. The notice informs users very little about what happens with their personal data:	The notice includes the information on how the rights may be exercised by the data principal and how

Na.Vijayashankar (Naavi)
37, Ujvala, 20th Main, BSK First Stage
Bengaluru, 560050
Phone: 9343554943
E-mail: naavi@naavi.org : Web:www.naavi.org

The notice to be shown to users when obtaining consent is only required to state what personal data will be collected and for what purpose, unlike previous iterations of the bill, which required companies to state how long they will store data, if they will share it with third parties, where the data was collected from, details on any cross-border transfer of the data, etc. Additionally, companies are not required to publish privacy policies on their site as required by previous iterations of the bill.	complaint can be made besides the indication of the purpose. There is therefore a means of collecting the information about how the data will be processed which will be of interest only to a class of information hunters and not ordinary data principals. The Consent managers will also be able to contribute in this regard to prevent any misuse. The DPB has to act either through its own monitoring or when non compliance is brought to their attention. Hence Objection is not relevant
9. No clarity on what safeguards companies have to implement to protect from data breaches: The DPDP Bill requires companies to take "reasonable security safeguards" to prevent personal data breaches and failure to do so can attract the highest band of penalty of up to Rs 250 crores. But there is no clarity on what measures should be taken and what constitutes as "reasonable" safeguards	There are different frameworks such as PDPSI or ISO 27001/27701 for the purpose. Hence Objection is not relevant
10. No compensation for victims of personal data breaches: While the Data Protection Board can impose a penalty of up to Rs 250 crores on an entity for a personal data breach, none of this goes towards the user, who is the victim of the data breach. Additionally, the Bill removes section 43A of the IT Act, 2000, which provided for such compensation.	This law is meant to discipline the industry. There are other laws to impose civil penalty or criminal punishments. Section 43 of ITA 2000 can be used to claim damages through adjudication under ITA 2000 since data principal can consider any damage suffered to him as a contravention of Section 43. Simultaneously Section 66 of ITA 2000 also can be invoked. Hence Objection is not relevant
11. The Data Protection Board will be a puppet of the government: The Chairperson and Members of the Data Protection Board will be appointed by the Central Government on terms specified by the government, raising questions about the Board's independence from the government. For instance, if the Board has to investigate a misuse of personal data of the government, there will be a conflict of interest because the government is essentially the judge, jury, and executioner of its non-compliance.	This is a speculative statement. The DPB will have members and Chairman who should be professionals and not become puppets by choice. There is a criteria for appointment and just as appointment or extension of terms of ED/CBI officials are routinely debated at the Supreme Court, every appointment in DPB is also justiciable. Hence Objection is not relevant.
12. Penalties for users for failing to fulfil duties:	This is required to ensure that Andolan Jeevies donot hijack the operation of the law.

Na.Vijayashankar (Naavi)
37, Ujvala, 20th Main, BSK First Stage
Bengaluru, 560050
Phone: 9343554943
E-mail: naavi@naavi.org : Web:www.naavi.org

The DPDP Bill allows the Data Protection Board to levy a penalty of up to ₹10,000 if a user fails to perform their duties as listed in the Bill. One of the duties, for example, is that users should not register false or frivolous grievances or complaints with a Data Fiduciary or the Data Protection Board. This provision could deter users from filing complaints in the first place in fear of a fine. A bill that's about protecting the right to privacy of users should not be levying any penalties on users.	If false and frivolous complaints are made then the DPB should have the discretion to impose penalties just as Courts impose costs on frivolous PILs. Hence Objection is not relevant
13. Exemptions for the use of personal data for debt recovery need safeguards: There are some exemptions granted to personal data processed for debt recovery. For example, if a person takes a loan from a bank and defaults on their monthly instalment, the bank may process the personal data of the individual to ascertain their financial information and assets and liabilities. Without any safeguards, this can be problematic as we frequently see instances of fake loan apps engaging in unethical recovery practices by accessing contact lists and photo libraries of borrowers and blackmailing them using this personal data.	This is another speculative objection without basis. DPB should be trusted to adopt guidelines to prevent any misuse of the law either to hide an offence or misuse of personal data. Unethical recovery practice is the domain IPC and not part of DPDPB as long as DPDPB is not a hindrance to the operation of IPC. Hence Objection is not relevant
14. No safeguards for sensitive and critical personal data: Certain types of data such as health, biometric or financial personal data merit stricter conditions for processing and storing. Earlier iterations of the bill had sensitive and critical personal data as subsets of personal data that were subject to additional safeguards. Such classifications don't exist in this bill.	Classification of data fiduciaries as "Sensitive" can address this requirement. All Significant Data Fiduciaries need to conduct periodical audit besides external data audit and have a DPO to assist the compliance. Hence Objection is not relevant
15. Does not apply to anonymised data: The law will not apply to anonymised personal data, which could be a problem because not only can anonymised data be deanonymised but it can also be layered on top of personal data to draw inferences of individuals.	It is well understood that Anonymised data is not personal data. De-Anonymization is a Cyber Crime and is covered by Section 66 of ITA 2000. Hence Objection is not relevant