GNI Comments to the Draft India Digital Personal Data Protection Bill, 2022

I. Introduction

The Global Network Initiative (GNI) welcomes this opportunity to provide input to the Ministry of Electronics and Information Technology on the draft Digital Personal Data Protection Bill, 2022 (the "DPDP").

GNI is a multistakeholder initiative that brings together over 85 prominent academics, civil society organizations, information and communications technology (ICT) companies, and investors from around the world. Members' collaboration is rooted in a shared commitment to the advancement of the GNI Principles on Freedom of Expression and Privacy and the UN Guiding Principles on Business and Human Rights (UNGPs). For over a decade, the GNI Principles and corresponding Implementation Guidelines have guided ICT companies in their assessment of risks to freedom of expression and privacy and responses to relevant laws, restrictions, and demands.

GNI acknowledges and appreciates the importance of the secure collection, storage, and retention of personal data, and the need to consider the potential human rights impacts of GNI members' practices in these areas, wherever they operate. GNI company members commit to disclose to users in clear language what personal information they collect, as well as policies and procedures for responding to government demands for personal information. They also commit to assessing, on an ongoing basis, measures for transparency with their users on their data collection, storage, and retention practices.

We write to express our concerns regarding some of the elements of the bill that undermine its admirable data protection aims, which we believe could raise challenges for companies seeking to protect user privacy. We also encourage MeitY to reconsider some of the exceptions that the DPDP allows for public actors' own data processing and collection. We are concerned that these exceptions, when taken together with other proposed and recently enacted provisions of Indian law GNI has commented on separately, pose real concerns for individuals ' privacy. We would also encourage stronger independence and oversight of any regulatory bodies tasked with enforcing the DPDP, and improved opportunities for redress for individuals whose privacy rights are affected by companies and the state.

II. Broad exemptions & limited accountability for government data collection & processing

The DPDP gives the government broad capabilities to exempt any of its entities and certain data fiduciaries from the prescriptions of the Act, with little to no guardrails, standard procedures for doing so, or forms of accountability. The lack of safeguards makes the exemption process vulnerable to abuse. This is a step backwards from previous versions of the bill, which allowed for exemptions only after a procedure that ensured the exemptions were fair, reasonable, and proportionate and pursuant to law.

The collection and processing of data by state actors should be subject to clear standards and meaningful safeguards set out under the Act. Any exemptions must be narrowly defined, subject to the principles of necessity, proportionality, and legality consistent with international human rights standards. This existing lack of provisions on oversight and accountability for access to data by public actors is a missed opportunity to help ensure more necessary and proportionate measures for government access to data in India, and to build public trust and confidence.

Specific provisions of concern include:

- Section 18 (2)(a): "The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data: by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these."
- Section 18 (3): "The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6 [giving notice], sub-sections (2) and (6) of section 9 [making sure data is accurate & retention restrictions], sections 10 [processing data of children], 11 [Significant Data Fiduciary rules] and 12 [rights of data principal to ask information from Data Fiduciary] of this Act shall not apply."
- Section 18(4): "The provisions of sub-section (6) of section 9 [ensuring data is only retained for as long as warranted] of this Act shall not apply in respect of processing by the State or any instrumentality of the State."

III. Deemed Consent

The Bill sets out a number of broad circumstances under which a data principal is deemed to have given consent for the processing of her data under section 8. Many of these are circumstances that are prone to abuse due to power dynamics between data processors and

principals, exposing the data principal to potential privacy harms without the ability to seek redress. For example, this includes:

- section 8(9): "for any fair and reasonable purpose as may be prescribed after taking into consideration:…**(b) any public interest in processing for that purpose…"**

Furthermore, under 2(18) of the Bill, "public interest" means in the interest of any of the following:…(f) **preventing dissemination of false statements of fact.** While addressing false information may be a worthy objective in certain circumstances, there is no clear justification for providing such broad license to disregard data protection for such a broad and subjective purpose.

IV. Data Protection Board independence

Under the DPDP, the powers and composition of the Data Protection Board are open-ended and pursuant to further definition by the Central Government, raising concerns about whether the DPB will be independent, and what its ultimate powers will be. It is critical that any oversight mechanism is independent, has a clear and transparent mandate, has proportionate powers, and is accountable. As noted earlier by GNI in the context of content regulation, to the extent substantial rule-making authority and discretion is delegated to independent bodies, robust oversight and accountability mechanisms need to be created to ensure that such bodies act pursuant to the public interest and consistent with international obligations.

Relevant provisions include:

- Section 19 (2): the composition of the DPB, its "strength" and selection process—are "as may be prescribed".
- Section 20 (1) (b): the DPB will "perform such functions as the Central Government may assign" through the Act or other laws.

V. Lack of rulemaking transparency

A number of provisions in the DPDP are left to be defined at a later date, as evidenced by the numerous references to provisions that are applicable "as may be prescribed." This practice reduces the transparency of the law, creates uncertainty about the ultimate prescriptions, and concentrates power in the hands of the Central Government with insufficient accountability or oversight.

Relevant provisions include:

- Section 7(7): "the technical, operational, financial and other conditions for the registration of consent managers."

- Section 8(9): “any fair and reasonable purposes for which a Data Principal will be deemed to have given consent to the processing of her personal data.”
- Section 10(2): “processing of personal data that is likely to cause harm to a child”
- Section 19(2): “the strength and composition of the Data Protection Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members”
- Section 19(4): “The terms and conditions of appointment and service of other officers and employees of the Data Protection Board”
- Section 17: “The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.”
- Section 11(2)(c): Significant data fiduciaries must “undertake such other measures including Data Protection Impact Assessment and periodic audit in relation to the objectives of this Act, as may be prescribed. For the purpose of this section, “Data Protection Impact Assessment” means a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed”.
- The notice for the submissions published by MEITY states that the submissions will not be made public, which further undermines the law’s transparency and legitimacy.

VI. Data Principals’ harms, rights, and penalties

While Chapter 3 of the Bill enumerates some rights for the data principal, a number of rights that were in previous versions have been removed. Importantly, this includes the right to access, the right to clear communication, the right to object, and the right to data portability. We appreciate that the Bill includes additional opportunities for grievance and remedy for users’ whose privacy rights may be affected, but additional “duties” for data principles listed in section 16 may actually undermine these opportunities for redress. These duties come with penalties of up to 10,000 rupees if not respected. This is a new and troubling development that could penalize data principals for attempting to control or retain their data and chills the data principal’s ability to exercise their rights under the Puttaswamy judgment. This includes requirements that data principals shall:

- Comply with provisions of all applicable laws
- Not register false or frivolous grievances or complaints
- Furnish any false information or impersonate another person
- Furnish only information that is verifiably authentic when exercising right to correction or erasure

In contrast to the previous version of the Bill, the DPDP removes the recognition of surveillance as a potential harm for data principals. When read with the broad exemptions that can be made under section 18 *“by any instrumentality of the State in the interests of sovereignty and integrity*

of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offense relating to any of these" the removal of this harm is concerning and further limits the redress an individual can seek if they are unlawfully surveilled by the government. Redress for unlawful surveillance is already a challenge as a result of provisions under section 69 and associated rules of the IT Act which prohibit the disclosure of government surveillance orders.

VII. Conclusion

As it currently stands, the DPDP raises several concerns for GNI. The broad exemptions for state access to and processing of personal data, the broad circumstances under which consent is deemed to be given, the dilution of data principals rights, the lack of transparent rule making, and the potential lack of independence of the Data Protection Board are all aspects that we believe could have significant negative and avoidable consequences on the privacy rights of data principals. If enacted in its current form, the DPDP will be a missed opportunity for the Indian government to align its practices on digital rights with international human rights standards and will undermine its international commitment to and reputation for upholding privacy online. GNI urges the Government of India to revise the DPDP to address these concerns and engage in further consultation with academia, civil society, and potentially impacted companies. As always, GNI stands ready to facilitate and support such engagement.