March 2025

Ministry of Electronics and Information Technology
Lodhi Road, New Delhi

Comments on the Draft "Digital Personal Data Protection Rules, 2025"

Thank you for the opportunity to comment on the draft of the "Digital Personal Data Protection Rules, 2025". We are researchers studying computer security as it relates to issues of public policy. We are offering some comments on the draft rules expressing our concern that they give the central government large, unchecked powers to request data from any intermediaries. This is a threat to the right to privacy under articles 14, 19, and 21 of the constitution.

Section 22 of the draft allows the central government to require any DF or intermediary to disclose information about a data principal "in the interest of sovereignty and integrity of India or security of the State". According to the seventh schedule, the State may use this data for "any function under any law" or to fulfill "any obligation under any law". These overly broad justifications gives the central government enormous powers and require a very low standard to be applicable. Additionally, the rules also allow the government to restrict the disclosure of the data sharing under similarly broad conditions, which means that there could be no transparency in the process. As they stand, the provisions of the DPDP act would allow the central government to perform unchecked surveillance.

While it may sometimes be necessary to compromise a user's fundamental right to privacy for a compelling state interest, we believe that the framework that grants the central government these powers should be robust against abuse. One of the issues that must be addressed to prevent abuse is to limit the scope of scenarios for which the government may request the release of data. This would require developing a framework to explicitly specify the limited settings where the government may request a data fiduciary for data about a data principal in line with the Right to Privacy verdict c.f. *Puttaswamy v. Union of India*.

To keep the government accountable, we recommend that the judiciary be required to issue **warrants** before the central government can exercise its powers to request data about a DP under section 22 of the rules. Under such a system, the restriction of data sharing disclosure would require the central government to sufficiently justify the necessity of that restriction. Additionally, to prevent indefinite, unnecessary restrictions of data sharing disclosure, warrants must always be **authorised only for a limited time period** that is no longer than strictly necessary. Should it later be necessary to extend the restriction, the government would have to seek another warrant justifying that extension. Once this time period expires, the DP should receive a copy of the warrant in addition to a notice from the DF.

To further enable accountability, we propose allowing data principals to retroactively file **appeals** to the judiciary against warrants for their data. This mechanism, together with consequences for data release requests that are later found to be unjustified, would help ensure that the government reaches for this tool only when absolutely necessary and defensible.

We hope that the Ministry finds these comments valuable and considers making changes to address the

threat of unchecked government surveillance by restricting the scope of its powers and adding processes to improve transparency and accountability.

Sincerely,

Specter Lab
Georgia Institute of Technology