Yesterday, the Government of India shared a near final draft of its data protection law with Members of Parliament, after more than a decade of engagement from industry and civil society. This is a significant milestone for a country with the second largest population on the internet and where privacy was declared a fundamental right by its Supreme Court back in 2017.

Like the previous version of the bill from July 2018 developed by the Justice Srikrishna Committee, this bill offers strong protections in regards to data processing by companies. Critically, this latest bill is a dramatic step backward in terms of the exceptions it grants for government processing and surveillance.

The original draft, which we called groundbreaking in many respects, contained some concerning issues: glaring exceptions for the government use of data, data localisation, an insufficiently independent data protection authority, and the absence of a right to deletion and objection to processing. While this new bill makes progress on some issues like data localisation, it also introduces new threats to privacy such as user verification for social media companies and forced transfers of non-personal data.

As the bill is introduced and reviewed in Parliament, attention and action is needed on several provisions. Here are some highlights:

- **Exceptions for Law Enforcement and other government use:** The biggest concern in the new draft is the bill's expansion of the broad exceptions that were present in the 2018 draft of the data protection bill for the government processing of data. Crucially, the requirement that government processing of data be "necessary and proportionate" has been cut. Furthermore, a provision was added granting the government complete discretion to exempt any entity or department from any part of the law. This leaves the current legal vacuum around India's surveillance and intelligence services intact, which is fundamentally incompatible with effective privacy protection.
- **Independence of the Data Protection Authority:** The new law further reduces the powers and independence of the data protection authority (DPA) by significantly weakening the commission that will appoint the Chairperson and members of the DPA. Where the 2018 draft said that they were to be appointed by a diverse committee with executive, judicial, and external expertise, the new law limits this committee to members of the executive. As with the last bill, Adjudicating Officers are also appointed by the government. Together, this will make it much harder for the DPA to be empowered and effective as the entire governing structure will be appointed exclusively by the government.
- **Social Media User Verification:** In a move that will be disastrous for the privacy and anonymity of internet users, the law contains a provision requiring companies to provide the option for users to voluntarily verify their identities. This would likely entail users sending photos of government issued IDs to the companies. There are also reports that intermediaries will have to report accounts that do not verify themselves using

such procedures to the government, which could make them a target for government scrutiny and investigation. This provision will incentivise the collection of sensitive personal data from government IDs that are submitted for this verification, which can then be used to profile and target users. This is not hypothetical conjecture – we have already seen phone numbers collected for security purposes being used for profiling. This provision will also increase the risk from data breaches and entrench power in the hands of large players in the social media space who can afford to build and maintain such verification systems. There is no evidence to prove that this measure will help fight misinformation (its motivating factor), and it ignores the benefits that anonymity can bring to the internet, such as whistleblowing and protection from stalkers.

- **Forced Transfer of Non-Personal Data:** The law also mandates that certain companies can be forced to transfer non-personal data to the government for public good and policy planning purposes. Not only can non-personal data constitute protected trade secrets and the insights derived from such data be protected by intellectual property law, but turning over this information to the government also raises significant privacy concerns. Information about sales location data from e-commerce platforms, for example, can be used to draw dangerous inferences and patterns regarding caste, religion, and sexuality. The law should continue to focus on the protection of personal data and leave the regulation of non-personal data to an independent law.
- **Ambiguity in Implementation:** The 2018 draft clearly laid out the timelines for the creation of the data protection authority, the accompanying subsidiary legislation, and the date in which the law would finally be enforceable. The new law removes all references to this timeline and merely mentions that the Central Government may notify the enforcement of the law at its complete discretion, creating ambiguity and uncertainty in the ecosystem.

On a positive note:

- **Data Localisation and Cross Border Transfers:** In a positive move compared to the 2018 draft, the law relaxes data localisation restrictions and applies them to only sensitive and critical personal data (i.e., personal data can be transferred without restriction). For sensitive data, the data can be processed outside the country and there are also reciprocity based exceptions that allows even critical and sensitive data to be processed outside the country. However, sensitive data must be stored in India, and it continues to be hard to see this as anything other than an effort to make surveillance easier.
- **Right to Erasure:** In a positive move, the new law includes an explicit right to erasure along with the right to correction, which gives data principles the right to demand that fiduciaries delete data which is no longer necessary for the purpose for which it was originally processed.
- **Strong obligations on companies and rights for individuals**: Over-

all, the bill retains the strong protections in regards to processing by companies that existed in the 2018 draft. In particular, there are strong provisions on consent, authorized basis for processing, purpose limitation, collection limitation, notice, data retention, data quality, data security safeguards, right to access, right to correction, data portability, and enhanced obligations for significant data fiduciaries.

Overall, while there are several strong provisions, significant concerns remain with the law and the Parliament will be critical in ensuring that Indians receive the data protection law they deserve. Mozilla will continue to engage with the Parliament, the Government of India, and other stakeholders over the coming months to help make this happen.