



Aug 20, 2020

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Data Privacy Detective Podcast – Episode 51: Non-Personal Data – India Stakes a Claim on Owning and Regulating NPD

A July 2020 Indian Government Report calls for regulation of Non-Personal Data. Most data privacy laws aim to protect (or not) personal data of people, This Report raises the question whether the world is about to see an explosion of regulation of non-personal data, which could change the business of data and how information flows within and across national borders.

Stephen Mathias, head of the Bangalore/Bengaluru office of Kochhar & Co., one of India's largest law firms, first updates us on two ongoing data privacy topics and then explains a novel approach to non-personal data being considered by the world's largest democracy.

The Personal Data Protection Bill is advancing toward adoption by the Indian Parliament. Patterned on EU principles, the Bill if adopted in its current form would align India generally with GDPR concepts, though with a data localization approach different from EU rules for data sharing across borders.

In August 2020 the Modi Government decreed as an emergency measure a ban of certain Chinese apps, grounded in concerns about how the personal data of Indian residents could be provided by the businesses with Chinese authorities. India joins the U.S. in using data and technology as a geopolitical tool against PRC actions that transcend data concerns. For Indian consumers and businesses that represent a large market for Chinese companies and provide services used by many Indian residents, this has raised a backlash from many using Chinese-sourced apps and concerns from businesses about the retaliation. Will trade wars be supplemented by data wars? Stay tuned.

But the big news of summer 2020 is the July 12 Report by the “Committee of Experts on Non–Personal Data Governance Framework.” It proposes governmental management of NPD – non–personal data, including the creation of an NPD Authority. If the Report becomes law, India will stake its claim to ownership of Indian data and become the supervisor of data flows and data sharing currently left generally to the workings of the market.

The Report was drafted by a group of mostly government bureaucrats and a few industry professionals. It aims to define how NPD should be regulated and shared, with the focus on sharing rather than collecting. NPD is identified as consisting of three types – public, community and private. Public NPD is what it seems – public information such as what a government collects or generates. Private NPD is data about businesses and individuals – for individuals if the data is anonymized and so under Indian principles is not “personal data” (even though such personal data runs the risk of re–identification). Community data includes anonymized data but is less clear than the “public” and “private” categories, as it may apparently be either. Examples of community data are traffic counts or a medical database of population counts infected by a particular disease.

Any organization that collects and provides services using NPD would be defined as a “data business.” Each data business would be required to disclose to and register with a regulator as an NPD data business. Thresholds would be set for what data businesses must register.

The Report justifies regulation of Non–Personal Data on several grounds:

- “data sovereignty” – viewing NPD data as a national resource owned by the state, and thus subject to being freely available to the government and to compulsory licensing to others as the government decides
- beneficial ownership of community data, with a trustee vested with free ownership of such information and able to decide who gets access to it

- the origin of personal data that becomes anonymized, based on the concept that data about Indian citizens and residents must be protected by the Indian government even in an anonymized state.

Data custodians would be designated to hold NPD data and act in the best interest of data subjects. This has two principal motivations – to unlock personal data for India’s common good and to prevent imbalances caused by data collected and controlled by monopolies and giant tech businesses, most of which are not Indian owned or controlled.

While the Report does not list the grounds on which data can or should be shared, examples are provided by category. One basis for sharing is the “sovereign” interest, related primarily to national and local security concerns. “Public” purpose relates to stimulating Indian research and innovation, policymaking, better delivery of public services and similar purposes. “Economic” purpose concerns India’s interest in encouraging commercial competition, promoting India’s substantial data processing sector and ensuring a level playing field or at least providing for fair monetary consideration for data sharing.

Data sharing is considered in two ways. One is that of data businesses, which must share their data periodically with the new NPD Authority. It would decide what data is then shared with Indian citizens and Indian based businesses. The second is data not held by a data business – such as community data. Concerns about the commercial impact of this concept include what happens to individual bits of data that a data business aggregates and adds value to the database – must that be shared freely with government, which can then share it publicly with no price to be paid to the data business. What impact will this have on India’s substantial IT sector? Will foreigners’ data be governed the same as anonymized data of Indian citizens or will an exemption be provided, similar to how the data of non-Indian persons is exempted by the current draft of the Personal Data Protection Bill?

The Report is just that at this point, with public comment sought by September 12, 2020. The legislative process will then begin its slow grind, with no law likely to be adopted for months or years. But the

Report is likely to stimulate similar thinking by other governments. Any “data business” should consider the Report and how it may shape regulation of what is currently considered a private matter. Data privacy is no longer only about personal data. It’s about the flow of all information, how it is collected, held, processed, shared, protected, and shared.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.