Moving towards a user data rights regime

The collection and use of personal data in order to deliver public and commercial services is now routine in India. For a country with large digital ambitions, one of the key questions will be: How should we think about regulating the use of Indians' personal data?

We believe that like rights to most goods, personal data will be best protected by a system of user data rights. The objective of such a regime would be dual: to empower people to use their information as they desire and to protect people from undesirable harms. Rights jurisprudence stretches back several hundred years, but a pithy definition encapsulating our modern understanding of rights is found in the *Stanford Encyclopaedia Of Philosophy* which defines rights as "entitlements (not) to perform certain actions, or (not) to be in certain states; or entitlements that others (not) perform certain actions or (not) be in certain states". The underlying nature of this entitlement can be understood as freedom of two kinds: freedom to enjoy certain conditions (i.e. empowerment) and freedom from certain conditions (i.e. protections against harms).

The Supreme Court decision in the K.S. Puttaswamy case (2017) sits squarely within this understanding. It declares privacy to be a fundamental human right of Indian citizens—protecting us from undesirable privacy harms that result from disclosure of our personal details and empowering us by reiterating our right to determine what we disclose about ourselves in different aspects of our lives. The core of a new data protection regime for India must be built around a system of user data rights serving these dual objectives. Such an approach would trigger graded obligations and liabilities for entities using personal data.

The implied premises of several existing approaches to data protection are that of a "property-only" view that commodifies data to give users the illusion of control. This has led to the creation of the fiction that when users are given a voluminous legal notice and asked for consent through "I agree" buttons, they are in effect exercising their property rights to sell or trade their data in exchange for services. The limitations of this "informed consent" or "notice and consent" model are well established. We know that users face cognitive constraints in evaluating the costs and benefits of consenting to data collection and use, since the benefits to be had are immediate and the costs of sharing personal information are often not apparent. This means we cannot rely solely on consent, but consider other user data rights to control the flow of personal data.

We propose that the focus of our future regime should be a system of user data rights. These rights should build in features from a range of legal paradigms to empower and protect individuals. Property-like rights granting "ownership" over personal data can only be a starting point. To avoid reinventing the (broken) wheel, we must consider lessons from paradigms like intellectual property, moral rights and human rights. Intellectual property rights like copyrights allow holders to grant licences for use for limited periods—a device which could have relevance to data sharing protocols. Moral rights, which give authors the right to stop modifications of their work that could harm their reputations, could provide parallels when considering the distortion of personal data. Human rights paradigms have increased relevance with the growing interaction between our digital and physical selves, binding us closer to our personal information. The judgements in the Puttaswamy case embolden this view, placing, as they do, certain rights in relation to informational privacy within the realm of inalienable human rights which individuals even acting autonomously cannot discard or give up.

Borrowing from the entire universe of rights jurisprudence would also help us think creatively about liability frameworks and obligations for entities processing data. Consider, for example, the financial transactions of a person purchasing medication for a serious illness. She might be happy to have this transaction history stored with her bank, and used by the bank's personal finance

management tool to recommend a monthly budget plan. This use could be dealt with through property-like data rights. However, disclosure of these details to third parties or the public could have terrible consequences—from social shaming to implications for future employment. This could trigger stronger sanctions and remedial rights for the person underpinned by moral or human rights, especially if it results in privacy violations or discrimination.

In India, we are at a decisive moment for data protection regulation. The Supreme Court has recognized our fundamental right to keep certain information about ourselves private. A committee on data protection chaired by Justice B.N. Srikrishna is currently working on a framework for a wider law that will determine the granular data protections afforded to individuals. We believe that a system of user data rights will balance the reality of new technologies and increased data processing with the need to limit harms to individuals and society. The law that enshrines these rights must be in line with users' reasonable expectations about how their data will be used, and also identify harms to be avoided. While designing these user data rights, we must cast the net wide to gain insights from a range of legal paradigms rather than defaulting to the current, unsatisfactory notice-and-consent-led model that neither empowers nor protects users.

Beni Chugh and Malavika Raghavan work at Dvara Research (formerly IFMR Finance Foundation).Comments are welcome at theirview@livemint.com

END