What the upcoming data protection law means

Data is the new oil, a mathematician famously said in 2006. Everything we do today with our internet-connected devices generates tonnes of data. By 2020, India will have more than 700 million internet users. But the country already has a burning need to come up with a world-class data protection and privacy law. There has been progress on this front and recently a white paper has been drafted by a Committee of Experts headed by Justice B.N. Srikrishna, set up by the Ministry of Electronics and Information Technology (MeitY). The recent Right to Privacy judgment of the Supreme Court and the Justice A.P. Shah Committee report on privacy have helped set the context for this white paper published on 27 November 2017 (read it here).

In India's financial technology space, innovations have been rapid, particularly after demonetization. As digital transactions rise, the country is now more receptive to innovations like eSign and eKYC via OTP through Aadhaar, which banks, insurers, fund houses and others use to onboard non-face-to-face customers. The Information Technology Act, 2000, provides for norms for data collection and its usage, but is silent on issues pertaining to the digital economy such as the definitions of 'data controller' or 'data processor' and their obligations, and it does not envisage the definition of 'consent' for data collection. Let's take a look at key aspects of the proposed framework, and what it means for the common person.

The white paper talks about strengthening existing standards for obtaining customer consent. It suggests that specific and separate consents should be obtained from the customer for usage of her data. And the consent should be 'explicit', 'given freely' and 'unambiguous'. The law must ensure that consent meets these broad criteria. For example, a business may require a customer's email ID, but the email ID must be collected with the customer's consent after having informed her of the use of it. However, these criteria should not end up in one standard fit-for-all model. For example, information that is not sensitive in nature may be categorized as low-risk and allowed to be collected by her implied consent. So, consent standards should align to the type or category of information being collected.

The data controller should only seek data relevant, commensurate and incidental to the service promised. The link between the services and the data requested should be clear and adequate in terms of 'minimum necessary'. Say, one installs a mobile app which optimizes phone battery performance. But the app wants access to media files, which it doesn't need. In setting the minimal consent standards, the law will have to decide whether the customer can bargain the degree of consent or be faced with a take-it-or-leave-it option.

The white paper reflects upon accountability as the central principle for data protection and delivery on the rights of the consumer. So the terms 'data controller' and 'data processor' get introduced. This would help determine accountability of each entity handling or processing data. Practically, the issue is in terms of who seeks consent and collects data, how she passes it to the processor or a third-party for processing or analytics, and where the identifiable data finally rests after the transaction. For example, you make a purchase on an e-commerce website whose data is stored on a third-party web-hosting service, and whose employee illegally accesses your credit card information. To address such complex issues of data collection, storage, processing, mining, and analytics, the law must clearly flesh out obligations, liability, and accountability by suggesting adequate regulations and minimum standards.

The Committee has proposed that data protection regulations should apply to both private-sector entities and the government but with differential obligations primarily depending on the nature and purpose of collecting or processing data. There will be limited embargo when it comes to the legitimate aims of state, national security, prevention of crime, and for disseminating social welfare

benefits. There are also exemptions contemplated for personal purposes or for journalism, artistic and literary work, academic research and statistical purposes. The level and scope of these exemptions are currently open-ended and need to be defined tightly to prevent misuse.

The law should prescribe best practices, and certifications to minimum standards for data protection techniques. The techniques of data anonymization (irreversibly preventing the identification of the individual to whom the data relates) and data pseudonymization (separation of data from direct identifiers so that linkage to an individual is not possible without additional information) should also be stressed on. It is better to have strict standards than remedial procedures and penalties for breach. The proposed data protection norms and safeguards are also going to increase the accountability of IT teams within various companies, and implementation of data protection framework could increase IT expenditure.

In line with similar legal provisions in jurisdictions such as the EU and Canada, the white paper envisions a right to be forgotten. It is said that once posted on the internet, nothing can ever be deleted. The white paper takes a balanced view of the right to be forgotten by saying it shouldn't impede the freedoms of expression and the Press. We will be provided a right to erase what we have posted online and even our entire online profiles, including data collected on us. But even the law may not be adequate to enable us to control the reactions of others to our online tweets and posts.

The Committee, while drafting the law, should not lose focus of the growing importance of a digitally driven economy. The law should consider the anticipated innovations in the digital finance sector and its contribution to the government's mission on Digital India and financial inclusion.

Parag Mathur is general counsel and head of compliance, Bankbazaar.

END