

Multiple scandals involving Facebook and Cambridge Analytica have made one thing clear – the failure of market forces to uphold privacy and protect user data. As long as there is demand for data, coupled with weak enforcement of laws, our privacy and data will remain vulnerable in the hands of private players. But it's not just the private sector, the Edward Snowden revelations were the key to unearthing the extent to which surveillance is entrenched in the systems of government which, in the absence of reform, will only expose our privacy and data to greater risk.

These are the fundamental concerns which justify the presence of a strong privacy regulator with effective independence and functional powers to enforce compliance. The regulator must necessarily prioritise user privacy above everything else because of the power dynamics and information asymmetry present today in how our data is treated. A practical illustration is when a service provider, public or private, may deny provision of a service in the absence of data, lowering the bargaining power of a user. Similarly, while consenting to give away data, users are not always aware of the full import of their consent. But the regulator, in enforcing best practices and monitoring compliance, is also promoting good business practices.

The Narendra Modi government last year appointed a committee under the chairmanship of Justice (Retd.) B.N Srikrishna, which has been tasked with the mandate of proposing measures to effectively address issues around data protection and privacy. This committee has also been playing with the idea of a regulator, possibly modelled on existing regulatory bodies like the Securities and Exchange Board of India or the Reserve Bank of India. As per some reports, the committee is expected to come out with its recommendations on June 18, following which a draft law will be put together.

The fact that the committee will propose a regulator is not surprising, rather it is the bare minimum. A law to balance rights and interests, in this case between data subjects and data controllers, cannot be successful in the absence of a regulator.

The points of contention, therefore, are the structure of such a regulator, its powers, its autonomy and the effectiveness of the processes. This is where, if the Srikrishna committee recommendations fall short, it will be a great loss to the momentous struggle in actualising the fundamental right to privacy.

Therefore, a group of lawyers, closely following the developments in this regard in recent months, have drafted the Indian Privacy Code, 2018, as a modest attempt at a model law, in which the idea of a strong regulator, a 'privacy commission', has been embraced.

**ALSO READ: [Spotlight on Srikrishna Committee, India's new data-privacy law: 10 points](#)**

It recognises and proposes some solutions to the implementation problem in a lot of our laws, taking off from SaveOurPrivacy's Seven Principles.

### **Strong, independent and effective**

Many discussions were held on how to realise the idea of a well-resourced body capable of handling the complex issues associated with the fragile right to privacy. Given the

geographical spread and federal nature of our country, the proposal included setting up of a privacy commission at the Centre and state privacy commissions in every state (with each state empowered through the code to establish such commissions in their respective states).

Here, three key considerations, of diversity, selection and independence of the 'privacy commission' went into the thinking and the drafting choices of the Indian privacy code.

**1) Diversity:** The commission is to be composed of a chief privacy commissioner and two privacy commissioners – with at least one commissioner with a judicial background and at least one commissioner to be a woman or member of third gender, or transgender. Commissioners need to imbibe integrity and exhibit ability in fields of privacy law and policy, business and human rights, civil liberties, data practices, technology and ethics etc. Since the concerns brought before the privacy commission are likely to be multifarious, it should also embody diversity of expertise and experience.

**2) Transparent selection process:** Privacy commissioners are to be appointed through issuance of a public advertisement, the responses to which will be screened by a search and selection committee, and will comprise judges, the law minister, opposition leaders, civil society, and other experts. The proceedings of the committee will be a matter of public record.

**3) Independence of the commission:** The code envisages that, given the crucial and often adversarial role that the commission will have to perform, independence from any external interference is non-negotiable. The security of privacy commissioners tenure is fixed, with a properly laid down removal procedure; their salaries and other emoluments have been pegged at par with other constitutional bodies like the Election Commission, and cannot be revised to their disadvantage; political appointments and people with business interests cannot be appointed as commissioners; Commission to have the freedom to decide the number and salaries of other officers and staff required to perform its functions effectively.

The code, however, doesn't prescribe a completely top-down approach for the regulatory framework. Each entity, dealing with data, is enjoined with a responsibility to appoint privacy officers in order to ensure compliance with the provisions of the code. For the compliant, the office of privacy commissioner will perform the function of an enabler and a guide. The idea is rooted in a business understanding that the cost of compliance is likely to be much less than the cost of damages payable and loss of reputation in case of breach. Similarly, any rule-making function of the privacy commission is to be carried out through a robust public consultation process, ensuring that multiple perspectives are accommodated in the best possible manner, without compromising on the principles laid down in this code.

**ALSO READ:** [We share limited data with Facebook to help customers, confirms WhatsApp](#)

The privacy commission, through its two composite offices – the office of data protection and the office of surveillance reform, each managed by a director general – will be equipped to perform the following functions, among others:-

Review, investigate or monitor, on its own or on a complaint made, proper implementation of the code and any digressions, adjudicate and pass remedial

directions including levy of fines and ensure speedy redressal of grievances;

Formulate norms and rules, through public consultation, for the effective execution of this code and advancement of privacy practices;

Undertake and promote research, training and capacity building in the field of privacy, data protection, surveillance and interception reforms;

Coordinate with state privacy commissions and other regulatory bodies;

Advise the central government on data adequacy status of other countries, in cases where data flows outside the borders.

## **Institutionalisation of Surveillance and Interception Reforms**

The code has also been premised on an understanding that any conversation on privacy is incomplete without adequate surveillance and interception reforms. Therefore, it envisages setting up surveillance and interception review tribunals in every high court, to be composed of two or more judges of that court. The tribunal will be empowered to review and either authorise or reject every order of surveillance or interception issued. The interests of the person to be surveilled or intercepted shall be defended through a panel of public advocates. The privacy commission, through its office of surveillance reform, shall also have a right to intervene to promote the cause of privacy and offer necessary assistance to the tribunal.

## **Oversight over the regulator**

Checks and balances are the hallmarks of democratic functioning of any institution and the code proposes the same for the privacy commissions. Any decision of the privacy commission shall be appealable before a designated bench of the Supreme Court (appeals from a state privacy commission shall lie before a bench of the high court of that state). Additionally, periodic reports prepared by the privacy commission, regarding its work and functioning, shall be laid before both houses of Parliament and an ad hoc committee of Parliament, comprising members from both Houses and chaired by the Lok Sabha Speaker, shall review functioning of the commission and table reports.

As India embarks on this ambitious project to codify norms for upholding privacy and data protection, it must be remembered that even the most well-meaning laws fail to deliver in absence of a strong body overseeing its enforcement. The experience with regulatory bodies in India may have been mixed, but that does not negate the need to have one or to propose a ‘facilitating’ body sitting on the fence as market forces bet on our data.

Having said that, all these proposed ideas are up for debate and deliberation and feedback and inputs are invited from the public to improve and strengthen the regulatory framework even further, so that it can best serve the interests of the people.