The Trilegal Technology, Media and Telecommunication Bulletin is a periodic update on recent developments in technology, media and telecommunications law and policy in India.

In January this year, the Government of India established a committee of experts on privacy, chaired by Justice AP Shah (**Shah Committee**) to review international best practices on privacy and recommend a framework for a privacy legislation in India. The recently issued recommendations contained in the Shah Committee report will serve as the blueprint for privacy legislation in India, a gaping void in India's legal regime that needs to be filled. The key recommendations of the Shah Committee have been analyzed below.

RIGHT TO PRIVACY

The Shah Committee recommends that the privacy legislation in India must statutorily establish a right to privacy to all individuals in India. It is recommended that the right be applicable to all situations, and must not require that a 'reasonable expectation' be present for the right to be invoked.

Limited exceptions have been contemplated. These include national security, public order, disclosure in public interest, prevention, detection, investigation, and prosecution of criminal offences, and protection of the individual or of the rights and freedoms of other individuals. The Shah Committee also recommends that the legislation must clarify that the publication of personal data for artistic and journalistic purposes in public interest, the use of personal information for household purposes, and the disclosure of information as required by the Right to Information Act, 2005 should not constitute an infringement of privacy.

While the Supreme Court has, on several occasions, articulated an implicit right to privacy derived from the language set out in Article 21 of the Constitution of India, a legislation that explicitly recognizes that right and sets out the contours of its applicability will go a long way towards developing the appropriate privacy jurisprudence.

PERSONAL INFORMATION

There is, at present, no law in India that protects the personal information of individuals. While certain provisions of the Information Technology Act, 2000 (**IT Act**) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011 (**IT Rules**) exist, these merely scratch the surface as they apply only to information on computer resources. Further, the IT Rules only protect the sensitive personal information or data, and not all personal information.

The Shah Committee does not provide a definition of 'personal information'. However, it recommends that any definition must be wide enough to take into consideration the contextual nature of personal information – the fact that the same piece of information can be personal in the hands of a certain data controller and functionally anonymous in the hands of another data controller.

For instance, the possession of a license plate number in the hands of an insurance company can be considered as personal information but the same plate number in the tape of a security camera in a petrol station will not be personal information. This recommendation, therefore, addresses invasions of privacy through collection of information that may not generally be regarded as personal information and hence could afford better protection of personal information.

APPLICABILITY

The Shah Committee also recommends that the privacy legislation must regulate not only personal information processed within India, but also personal information that originated in India and which has subsequently been transferred outside India. This stance appears consistent with the press note dated 24 August 2011 issued by the Government of India (**Press Note**) clarifying the applicability of the IT Rules that regulate sensitive personal information. The Press Note provided that the IT Rules apply only to persons or bodies corporate located in India, and not to persons or bodies corporate located abroad.

The Press Note also clarified that only a body corporate providing services to an individual under a direct contractual obligation in India would be subject to the IT Rules and consequently, the IT Rules do not apply to contracts between corporate entities even if they relate to the collection and use of personal information. The Shah Committee appears to be silent on whether the privacy legislation should have similar applicability.

NATIONAL PRIVACY PRINCIPLES

The Shah Committee recommends that this legislation must harmonize all statutory provisions that relate to privacy. To achieve this objective, the privacy legislation must provide for certain 'national privacy principles' in relation to collection, processing and transfer of personal information. The national privacy principles form the crux of the Shah Committee's recommendations, and also any privacy legislation that is drafted on this basis.

These principles are along the lines of those provided in the IT Rules in respect of sensitive personal information or data. The national privacy principles include chiefly, consent of the data provider prior to collection of personal data, choice to withdraw such consent, notice and information to the data provider at the time of collection, limitation of the use of personal information for the stated purpose, access to personal information for data providers and the ability to seek copies and make corrections, consent prior to disclosure, and implementation of security safeguards for protection of the information.

Crucially, it must be noted that these privacy principles will be applicable to the collection, processing and use of personal information, through any mode including interception, as well as audio and video recordings. The privacy principles shall also apply to collection of personal identifiers such as passports and PAN cards, as well bodily and genetic material from individuals. These principles will apply both horizontally as well as vertically – i.e., both to governmental organizations as well as private persons and corporate bodies.

REGULATORY MECHANISM

Perhaps the most daunting challenge of a legislation of this significance is to ensure that it does not remain a paper tiger. The legislation must, therefore, create robust regulatory and enforcement mechanisms. The mechanisms suggested by the Shah Committee have only been sketched out in scant detail, and will require further deliberation.

Privacy Commissioners

The Shah Committee recommends the appointment of a retired Supreme Court judge as a Central Privacy Commissioner, to oversee the implementation of the provisions of the privacy legislation. The Central Privacy Commissioner will further be assisted by several Regional Privacy Commissioners, who

will be retired judges of a High Court. The Privacy Commissioners shall be vested with the following powers:

- Conduct investigations into complaints of non-compliance of the national privacy principles.
- Examine and call documents, examine witnesses, and compel appearances.
- Impose fines on data controllers who are in contravention of the national privacy principles.
- Order privacy impact assessments in relation to implementation of the national privacy principles by data controllers.
- Review the working and functionality of the privacy legislation, and suggest amendments.

Self-Regulation

The Shah Committee also recommends empowering self-regulatory organizations at industry level to develop privacy standards for each industry with the assistance of the Privacy Commissioners. Any industry-specific standards will be approved by the Privacy Commissioners, and shall be at least as stringent as the national privacy principles. Once formulated and approved, the Privacy Commissioners shall be entitled to enforce the agreed self-regulatory standards.

In addition to formulating privacy standards, each self-regulatory organization shall also appoint an ombudsman who shall be empowered to receive complaints from individuals. The Shah Committee recommends that prior to approaching the Privacy Commissioners or a court, individuals approach the self-regulatory organizations for speedy resolution of a dispute.

Enforcement

The Shah Committee recommends a three-tiered approach to dispute resolution:

- Ombudsmen: It is recommended that each self-regulatory organization put in place an alternative dispute resolution mechanism to deal with complaints investigated by ombudsman to reduce dependency on the Privacy Commissioners and courts, and ensure expediency.
- Privacy Commissioners: Aggrieved individuals may also approach the Privacy Commissioners, who may investigate the complaint and impose fines.
- Courts: Individuals may also approach the court for any non-compliance with the national privacy principles, and the privacy legislation must empower the court to impose fines for any contravention.

CONCLUSION

The Shah Committee's recommendations provide the basis for the formulation of a much-needed national privacy legislation. It must be remembered that many of these, particularly those regarding regulatory and enforcement mechanisms, are only in the nature of broad suggestions. These recommendations, while foundational, will need to be carefully shaped into a statute. It is hoped that the report of the Shah Committee will act as a shot in the arm for the government, and a comprehensive privacy legislation will be introduced in parliament sooner rather than later.

If you require any further information about the material contained in this alert, please get in touch with your Trilegal relationship partner or send an email to alerts@trilegal.com.