Internet And Mobile Association Of India

IAMAI Position Paper on Privacy

IAMAI supports a legislative framework to help advance the right to privacy in India. It also submits that the interests of industry and that of users is complementary in ensuring a clear legislation which defines the treatment of personal data. The Association looks forward to further opportunities to engage and assist in providing inputs on any future privacy statute.

Need for public consultation

It is important to stress the need for an organised call for comments and public consultation prior to introduction of any bill in Parliament by the Government. This principle of consultation has been acknowledged by the Department of Personnel and Training earlier when it published its Approach Paper to Privacy. Further, the Department of Personnel and Training's notice refusing to extend the one week consultation period on the approach paper in November, 2011 had stated that the public will have an occasion to comment on any legislation if-and-when such legislation was decided to be enacted. Consultation becomes relevant given that importance to the Indian economy from business activities and technology development based on the collection and use of data. Any law regulating such concerns should account for the pace of flexibility and innovation in this sector. This is necessary given that the internet and mobile sectors have been a major growth sector in the Indian economy – with nearly 1.6 per cent of India's GDP already coming from the Internet alone, and projected to double by the end of 2015.

Even before the introduction of such privacy law, many cardinal principles and definitions need to be considered which have been highlighted. We would appreciate the opportunity to submit a more detailed information on each of them.

Definition of Data

Any definition of 'data' should reflect a recognition of the different forms of data. This would naturally include within itself the different gradations of data, such as Data, Personal Data and Sensitive Data. Further provisions should be made for Anonymous Data and Pseudonymous Data. A functional definition of personal data and what data is covered by various provisions of a law would be one that recognizes both context (what is known by the data controller that holds it, and what might a user reasonably expect) and identifiability (does the data, itself - using means reasonably available to the Data Controller - identify an actual person?). This same principle should be extended to data controllers whose status may define whether the same data is personally identifiable or mere data.

These gradations in the definition should ideally be mapped against the obligations which are put on data controllers with respect to each class of data. Ideally, the protections and duties which apply for sensitive data should be at a higher threshold when compared to personal data only.

Consent through notice

The basis of compliance in most privacy statutes is based on receiving informed consent. It is important that this be done through the provision of notice and choice to the users in an easily acceptable and practical manner recognizant of business practices and the innovation that technology products offer users. To commence the law should make it clear that requirements for "written explicit consent" - if and where required - include consent given via online agreements and other electronic methods.

Indigenous privacy approach

The drafting of a privacy law presents an opportunity to draft privacy definitions and a regulatory approach specific to India. In this respect the Justice A.P. Shah Committee on Privacy has analysed privacy standards which exist in foreign legislation and proposed by international organisations. This analysis is succeeded by certain common privacy principles which were proposed by the Committee. In this exercise the Committee has recognised the need for adaptation of existing international regulation to local suitability.

Most international regulation is at present fluid, where it can at best be used to draw a base line. For instance the EU Model of Privacy (Data Protection Directive, 1995) is itself under a process of review. The EU Model has in the past come in for criticism for making compliance complex due to its heavy handed approaches of prior approval of privacy impact assessments. IAMAI encourages an open minded approach to foreign legislations with a view to develop indigenous approaches - even with respect to the structures of such frameworks. A wider public consultation can help the process of finding a consensus amongst stakeholders.

Ex-post penalty

The general model under most Indian laws is towards imposition of liability towards breaches *after* breaches occur. An exception to this general rule is made in cases of environmental compliances or ultra-hazardous activities. In any event data which is gathered, stored or processed does not pose such risk. After suggesting minimum standards under a law, there should be no requirement to take approvals of an authority for the commencement of activity on a case to case basis. Such a process is likely to induce delay which may discourage innovation and the offering of digital services. In case of breaches the most appropriate remedy is monetary compensation which is discussed in further detail below.

Penalties for breaches

Keeping in view the horizontal approach of the proposed privacy law (i.e. it applies both to the State and the private sector), IAMAI recommends monetary civil remedies. An effective and efficient enforcement of privacy breaches by civil remedies will create the appropriate disincentives for non-compliance. An approach towards such civil penalties will serve the twin objectives of deterrence and compensation.

An approach towards enforcement through civil remedies also recognises that the basis of any privacy law is consent. Here the consent is signified through user agreements and contracts. Hence, the natural remedies which arise with respect the private sector are compensatory penalties.

The Federal Trade Commission in the United States has in the past filed complaints for monetary civil penalties under Sections 1303(c) and 1306(d) of COPPA and Sections 5(a)(1), 5(m)(1)(A), 13(b), and 16(a) of the Federal Trade Commission Act. Most of these complaints have been settled by private parties, which ranged for negligent disclosure to improper notices informing users of data collection.

Further, this will not foreclose criminal action which results from injury from the privacy breaches. For instance, the mere breach of the privacy law by unlawful disclosure would be dealt by compensation under the Privacy Law. However, the use of information to commit the offences of theft or a transfer of funds, would be covered by provisions of the Indian Penal Code, 1872. In the view of IAMAI this would reflect a correct balance of law, since news reports have only highlighted the negligence of BPO's and call centres with respect to disclosure of customer information. However, subsequent illegal activity where such information is used by former employees to siphon off funds is dealt effectively with prosecutions under the Indian Penal Code, 1872.

It is also the view of IAMAI that creation of criminal penalties and new offences for breaches of privacy is likely to discourage investment and development of business which relies upon collection or analysis of data.

Recognition for co-regulation

There is a need for any enactment to provide legal recognition of voluntary self-regulation. An instance is the Federal Trade Commission approved standards adopted under the Children's Online Privacy Protection Act (16 C.F.R. Part 312) ("COPPA"). Under COPPA rules enforcement is left to private stakeholders through government recognition and supervision. It is pertinent to stress that this model of prior approval of privacy programs under COPPA is provided since it targets information which is specifically gathered of children aged under 13 years.

Such an approach also marks a continuity from the rules made under Section 43A of the Information Technology Act, 2000. Specifically, Rules 8(3) and 8(4) provide for compliance through IS/ISO/IEC codes, failing which codes of best practices for data protection as notified by the Central Government may be adopted.

This approach is also recommended in the Justice A.P. Shah Report on Privacy which notes the role of "Self-Regulatory Organisations (SRO's)". It states in the executive summary that, "However, rather than prescribe a pure top-down approach to enforcement, this report recommends a system of co-regulation, with equal emphasis on Self-Regulating Organisations (SROs) being vested with the responsibility of autonomously ensuring

compliance with the Act, subject to regular oversight by the Privacy Commissioners. The SROs, apart from possessing industry-specific knowledge, will also be better placed to create awareness about the right to privacy and explaining the sensitivities of privacy protection both within industry as well as to the public in respective sectors."

This highlights that different sectors utilise different types of data. Depending on their sensitivity, industry privacy practices are developed specifically for such sector. This promotes efficiency and allows for flexible business models to account for technological development. It is suggested given the unique challenges which may arise in terms of granting approvals for such programs a regime of deemed compliance may be adopted. This will avoid bureaucratic structures and ensure that industry practices match the pace of technology. For instance the Central Government has till now been unable to formalise a structure or to notify any code for best practice under Section 43A of the Information Technology Act, 2000.

About IAMAI

The Internet and Mobile Association [IAMAI] is the representative body of internet and mobile data businesses. Its 130 members represent and service 137 million rapidly growing Internet and mobile data users in the country. This paper is prepared to cater to the needs and requirement of our consumers and our industry members.