Strengthening Privacy Protection through Co-Regulation

- **Prepared by Data Security Council of India**

Privacy and Self-Regulation

Voluntary disclosure of privacy policy was used by most organizations to reach out to the people that their Personally Identifiable Information (PII) was secure with them. Such statements merely reflected organizations' commitments to a set of Privacy Principles. It was in 1980 that OECD Guidelines on the Protection of Privacy and Transborder flows of Personal Data, in close coordination with the Council of Europe, were issued. In 1985, OECD issued another declaration on transborder data flows that dealt with data flows within transnational corporations, trade barriers, and related aspects of data protection, and envisioned better cooperation and harmonization. However, such commitments in the form "Codes" or "Guidelines" would indicate a self–regulatory function. The organization showed that it had considered privacy protection at some level; however, it was more in the nature of good public relations to state a set of commitments. Privacy commitments may inform data subject about certain rights to access and correction, to opt–out of disclosures, and so on.

Over a period of time, privacy codes of practice evolved, which were usually operating in absence of a regulatory framework. Some of these privacy codes graduated to the level of privacy standards, and ultimately resulted in the establishment of privacy laws. The first such code was the Canadian Model Code for the protection of Personal Information in September 1995, which was subsequently approved as a "National Standard of Canada" by the Standards Council of Canada in March 1996. The standard was organized around 10 Privacy Principles. Its development was led by the Canadian Standards Association (CSA) with very active participation of the industry; it was known as the CSA Model Code. Same course of events took place in Australia where the standard was based on the CSA Model around a set of National Privacy Principles in 1988. This was superseded by a Privacy Act later. In 1999, the Japanese Standards Association released JIS Q 15001, which adapted the Environmental Management Standard, ISO 14001 for personal data protection. This again led to the establishment of a Privacy Act in 2005. Privacy codes of practice are administered in these countries by the industry bodies in the co-regulation model.

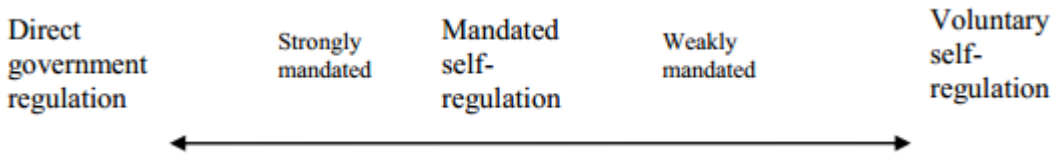
Codes of practice have long operated in various countries, as part of self–regulation. Five kinds of privacy codes, according to the scope of application, have existed: the organizational code, the sectoral code, the functional code, the technological code and the professional code. Privacy codes of practice differ from mere privacy commitments in that they may embody a set of rules for employees, members or member organizations to follow. They also provide important guidance about correct procedure and behavior based on the information privacy principles and procedures for implementation, complaint resolution, and communication.

Co-Regulation Regime

In the privacy led by business associations, enforcement in general is not very strict, but industry associations are playing an increasing role in educating their members about privacy based practices, through specialized seminars, training services, etc. This form of self–regulation more closely resembles the "managed compliance" approach than the enforcement approach. But if trade associations have mandatory membership, it can act as a strong support for self–regulatory privacy protection instruments.

The experience of Canada, Australia, Japan and the United States where privacy codes, privacy standards and privacy seals have been developed and implemented, have graduated to the level of becoming part of the privacy laws that have got created. However, all of them see the role of self-regulation as an important element in ensuring privacy. The experience supports the conclusion that the voluntary approaches are not something to be ignored, but rather an integral part of privacy.

Below line graph lists different type of possible regulatory frameworks:[1]



Voluntary self-regulation with legal recognition evolves into a co-regulatory regime, i.e., mandated self-regulation. It is a hybrid of two regulatory forms – Direct government regulation and Voluntary self-regulation. The Co-regulatory regime can be of different types based on the role played by the government and industry in rule creation and enforcement.

Regulatory Aspects	Government	Industry
Rule Making		
Enforcement		

The United States has a history of self-regulation and co-regulation: FTC-approved safe harbor programs under COPPA, and that of the Children's Advertising Unit (CARU) exemplify strongly mandated self-regulation, where industry is responsible for both rule making and enforcement, but under close government supervision; Network Advertising Initiative (NAI) Principles, which take the form of a weakly mandated self-regulatory scheme in which an ad hoc industry advertising group defines a set of governing principles (which the FTC informally approved) and also oversees members' compliance; North American Electric Reliability Corporation (NERC), which is responsible for establishing and enforcing standards for the electric power grid. NERC is certified by the Federal Energy Regulatory Commission.

[1] http://www.ftc.gov/os/comments/privacyroundtable/544506-00103.pdf

The EU-US Safe Harbor is another type of co-regulatory regime. To benefit from the safe harbor, US firms had to certify that they would comply with privacy principles negotiated between the US and EU, administered by industry seal programs created for this purpose by DMA, Truste, BBBOnline, and others. Thus, industry manages the enforcement of publicly-written rules but subject to weak government oversight. This arrangement combines transactional self–regulation on the one hand, and nation-state–based intergovernmental public regulation on the other, to produce a complex, multi-layered regime.

The EU Data Protection Directive—states that — *Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority* (Article 27 (2)). The proposed EU Data Protection Regulation also foresees ***drafting of codes of conduct covering various sectors,*** and allows them to be submitted to Authorities, which may give an opinion as to whether they are "in compliance with the Regulation" (Article 38(2)). Compliance with a code of conduct may be deemed to satisfy the legal requirements of the proposed Regulation. Article 39 establishing ***"data protection certification mechanisms and of data protection seals and marks"***, is encouraged, though the legal effect of such recognition needs to be clarified.

The European Union Directive encourages co-regulation and the national data protection laws of several European countries follow this approach. The United States, of course, is known to support co-regulation. Australia, Canada and Japan have privacy laws, but they recommend the adoption of model privacy codes that are recognized by the laws. ***A single privacy regulator in any part of the world cannot protect privacy of individuals*** *- not only of its citizens, but also of the personal data that flows from other countries, as part of global data flows in the networked environment, which is only bound to increase further with the passage of time.*

In India, **sec43A of the IT (Amendment) Act, 2008 recognizes co-regulation**. Clauses (3) and (4) of Rule 8 of sec 43A state:

Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC ***codes of best practices for data protection*** *as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.*

The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the ***codes of best practices for data protection*** *as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government.*

Co-Regulatory Enforcement Regime as recommended in the Justice A P Shah Report: The report recommends the establishment of the office of the Privacy Commissioner, both at the central and regional levels. The Privacy Commissioners shall be the primary authority for enforcement of the provisions of the Act. However, rather than prescribe a pure top-down approach to enforcement, this report recommends a system of co-regulation, with equal emphasis on 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 recommendation of a co-regulatory regime will not derogate from the powers of courts which will be available as a forum of last resort in case of persistent and unresolved violations of the Privacy Act. ***SROs will be responsible for appointing an ombudsman to receive and handle complaints***, and will be responsible for promoting education and awareness of sector specific privacy standards.

Data Controllers and Privacy Officers: Every organization which determines the purposes and means of processing personal information will be considered a data controller. Data controllers will be responsible for carrying out the processing of data in accordance with sectoral privacy standards or the national privacy principles. ***If a particular sector/industry does not have an SRO, then data controllers from that sector/industry will have to comply with the National Privacy Principles supplemented by any specific norms/standards prescribed by the Privacy Commissioner***. These norms/standards may include the appointment of an organisational level privacy officer for complaints to be raised to and resolved. The appointment of privacy officers is meant to reduce case pendency in courts and at the regulators' office as well as to provide quick remedy/relief to consumers and citizens.

DSCI Recommendations for the Proposed Privacy Law

(i) Have ***light weight regulations*** based on global privacy principles that ***value economic benefits of data flow and usage, while guaranteeing privacy to citizens***

(ii) ***Avoid bureaucratic structures*** that could hinder business interests and lose the spirit during implementation such as creation of a Data Protection Authority - No single authority can ensure effective enforcement of regulations across different industry verticals in such a vast country.

(iii) ***Rely on self-regulation of businesses*** that promote practices, ***making the privacy program relevant to technology advancements***

(iv) Provide ***legal recognition to the role of self-regulatory bodies***, promoted by industry associations, in enforcing privacy codes in the interest of citizens' rights

(v) Create regulatory structure that provides ***right incentives for organizations to do privacy***

(vi) Establish a mechanism, in the form of ***public private partnership***, to ***resolve the disputes and grievances of citizens***

(vii) ***Promote trans-border data flows instead of hindering them,*** as these flows contribute a lot to the economy of nations.

(viii) Create provisions for continuously enhancing ***end user education and awareness on Privacy.***

At this stage we should identify privacy principles; ways to enforce them; promote co-regulation through codes of conduct in sectors/industry verticals; create awareness and educate government and industry in sensitivities associated with privacy protection; promote the growth of privacy professionals; integrate with growing digital economy even as we protect the privacy of our citizens and consumers. Co-regulation should be encouraged to achieve higher level of compliance, since it is only the industry verticals which can undertake the responsibility of creating awareness in their respective sectors – this is critical for the successful implementation and enforcement of the proposed privacy law. The SROs will define the process and codes of practice, which are vetted and recognized by the government through the proposed privacy law. Co-regulation should be the guiding spirit.

Discussion Points

1. What roles should government and industry respectively play in rule creation and enforcement? (weak mandated self-regulation v/s strong mandated self-regulation)
2. How can the codes of practice be enforced in a co-regulatory regime? How will the SRO check the successful implementation of codes of practice (Audits/ Privacy Seals etc.)? How can the SROs penalize non-compliances?
3. How can the organizations be incentivized to follow the codes of practice under the SRO?
4. What should be the role of SROs in complaint redressal?
5. What should be the business model for SROs? Who should bear the expenses of investigations?
6. How will co-regulation work in sectors where there are no industry associations or SROs?