THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

Outsourcing In India: Designing A Privacy Accountability Self-Regulatory Organization

June 2007

Background

With the growth of the Internet, global markets, and consumer expectations for services and assistance 24/7, businesses now move data to locations worldwide for data processing and management services. Since the 1990s, India has been a destination market for outsourcing and business process support for global companies. Its educated workforce and progressive democracy makes India a particularly attractive location for these services, and today nearly 65 percent of all outsourcing occurs in India.

Recognizing that appropriate protections for the security and privacy of data are critical to the continued growth and success of the outsourcing industry, India has taken measures to implement data controls. In response to noted breaches of data security that have been reported in connection with outsourced services to Indian companies, India's government has approved security enhancement proposals. It has also recommended legislative enhancements to the Information Technology Act of 2000 that would strengthen enforcement tools and require corporate accountability processes for data privacy and security. The draft legislation calls for the development of internal and external best practices and guidelines as part of each company's commercial security and communications policy.

The Indian government's proposed legislative enhancements are consistent with continuing efforts of India's IT sector to strengthen the privacy and data security practices of the country's business process outsourcing companies. The National Association of Software and Services Companies (NASSCOM), an Indian IT trade association, launched two self-regulatory initiatives this past year to encourage privacy and data security accountability in business processing outsourcing.

NASSCOM announced the creation of the Data Protection Council of India, a self-regulatory organization (SRO) for the industry. The Council will set standards for privacy and data security, and will monitor its members to help ensure that they adhere to the standards. The SRO would have enforcement authority over its members and could take certain corrective actions upon learning of a data breach by a participant company, including referrals for government enforcement actions. The SRO would also assist companies in reaching compliance with the standards through education, awareness-building and training.

At the same time, it is important that the SRO for the outsourcing industry be sufficiently flexible to respond to changing business models, technical requirements and data flows. Principles developed in the Asia Pacific Economic Cooperative forum on privacy could serve as a central model for such a mechanism, as they reflect the international nature of data flows, and anticipate the need to honor the privacy and security commitments and protections afforded data by its country of origin, regardless of the data's ultimate destination or processing location.

The Project

Partnering with the US-India Business Council leaders from across US and India business sectors, NASSCOM invited The Center for Information Policy Leadership, affiliated with Hunton & Williams, to join in the dialogue that will assist industry leaders in the development phase of the SRO. The Center for Information Policy Leadership will provide guidance on building sustainable privacy accountability into outsourcing relationships according to international standards, including the principles developed in the Asia Pacific Economic Cooperation forum.

The effort will develop standards to ensure that data is processed in India securely and consistent with the promises made when the data was collected by the business customer of the outsourcing provider. Under the self-regulatory organization framework, privacy accountability will be closely and vigorously regulated by industry and accountability agents to maintain trust and confidence in outsourcing services. The recommended framework will also reflect the dynamic nature of global data flows and the need to respect the privacy and security requirements of information regardless of its origins without placing additional demands upon outsourcing providers.

The Center for Information Policy Leadership's India self-regulatory organization project is a non-core project supported by Center member and non-member companies.

The project will:

- Review the initial self-regulatory organization proposal;
- Draft a straw-person self-regulatory organization roadmap;
- Revise the roadmap based on member input; and
- Create a final version of the guidance.

For more information contact Maureen Cooney (mcooney@hunton.com; 202.955.1517), Marty Abrams (mabrams@hunton.com), or Paula Bruening (pbruening@hunton.com).