

**WILL THE PROPOSED AMENDMENTS TO INDIA'S INFORMATION
TECHNOLOGY ACT, 2000,
RESOLVE DATA PRIVACY ISSUES?**

Data privacy and security are the biggest concerns for international clients outsourcing to India. To address this, the Ministry of Communications and Information Technology, Government of India, proposes to amend the Information Technology Act, 2000 (the "ITA"), to include stricter provisions for data security. On October 16, 2006, the Cabinet of Ministers accepted most of the proposed amendments, and the bill to amend the ITA will be presented in the Parliament in the winter session.

Liability of BPO companies for data theft

Under the ITA, an intermediary (including a BPO Company) is liable for data theft, unless it proves that it did not have any knowledge of the contravention committed, or that it exercised complete diligence to prevent the commission of such an offence or contravention.

However, the bill to amend the ITA has raised the bar for BPO liability. The proposed amendment suggests that an intermediary will not be liable for data theft in respect of any third party information or data made available to it, except where the intermediary conspires or abets in the commission of the unlawful act. Moreover, this will not apply if, upon receiving actual knowledge, or being notified by the Central Government or its agency that any information or data residing in a computer resource controlled by the intermediary is being used to commit data theft, the intermediary fails to expeditiously remove or disable access to that material in that resource.

This implies that an Indian BPO company will not be liable for any third party data theft unless the foreign firm, whose data has been stolen, is able to substantiate that the Indian BPO company conspired or abetted in such activity. Although this provision is beneficial to Indian BPO companies, it will not help foreign companies outsourcing data to India as they will have to prove abetment or conspiracy of the Indian BPO companies.

Further, if an intermediary, who has secured any personal material or information from its subscriber / user, with an express or implied promise of confidentiality,

discloses such information or material to any other person, without the consent of such subscriber / user and with an intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation up to Rs. 2,500,000 (US\$60,000 approximately) to the subscriber / user so affected. For example, if a bank discloses the personal information of any of its customers to a third party without the consent of the customers and with the intent to cause injury to the customers, the bank will be liable to pay damages up to Rs. 2,500,000.

Liability for inadequate data security

Another proposed amendment seeks to make companies liable for negligence in maintaining appropriate security practices. Accordingly, if a BPO company is found to be negligent in maintaining reasonable security practices with respect to sensitive personal data or information of third parties in a computer resource that it owns or operates, it shall attract damages by way of compensation up to Rs. 50,000,000 (US\$1,100,000) to the person affected. Therefore, Indian BPO companies will have to put in place adequate security practices and procedures and will not be able to shrug off this responsibility. The amendment also permits companies to agree on security measures contractually. As such, a foreign company outsourcing work to an Indian company should list out in the contract, the specific security management standards and procedures to be adopted by the Indian company with which it enters into the services contract.

Although this is a very positive amendment, the maximum compensation of Rs. 50,000,000 may be inadequate as compared to the value of the data stolen due to such negligence.

Hacking

Currently, the ITA divides illegal cyber activity into cyber contraventions, which entail civil liabilities, and cyber crimes, which entail criminal liabilities. However, a proposed amendment recommends that cyber contraventions should also entail criminal liability, if these are done with a dishonest or fraudulent intention. In other words, cyber contraventions are proposed to be brought on par with cyber crimes if they are done with a dishonest or fraudulent intention. Thus, acts like hackings, accessing any computer resource, downloading, copying or extracting any data, etc., when done by an unauthorized person with a dishonest or fraudulent intention, will entail criminal liability. The intention of the Indian government is to

increase the gravity of the offences to dissuade people from engaging in such crimes.

The proposed amendments need to be tweaked slightly to give comfort to foreign clients outsourcing to India. For one, the Rs. 50,000,000 limit on damages should be withdrawn, and there should be no cap at all. This is because foreign banks and companies may face much higher liability in their home countries from their customers if customer data is stolen from an Indian BPO company in breach of security and other guidelines.