Recent amendments to Indian IT law

By Priti Suri and Mahendra Singh, PSA, Legal Counsellors

PSA
Legal Counsellors
E-601 Gauri Sadan, 5 Hailey Road
New Delhi - 110 001, India
Tel: +91 11 4350 0500
Fax: +91 11 4350 0502
Email: p.suri@psalegal.com

The Information Technology Act, 2000, came into force on 17 October 2000. As IT by its nature is continually transforming and reinventing itself, it is necessary to periodically take a fresh look at any IT-related law. Rising concerns in the last few years – about data security, data privacy, hacking, child pornography, spam, phishing and other online offences – gave rise to the need for the IT act to be revised.

The IT act review process began with the setup of an expert committee in January 2005, and culminated on 5 February with presidential assent of the amendment bill and the entering of the Information Technology (Amendment) Act (ITAA), 2008, in the statute book. The ITAA, which is yet to come into force pending finalization of the draft rules and issuance of the necessary notification, introduces significant changes:

Data protection: To satisfy a long-felt need to protect confidential information handled by the business process outsourcing (BPO) sector, the ITAA formally introduces the concept of data protection through two new sections, 43A and 72A. These provide for civil and criminal liability for failure to protect personal data and impose strong obligations on Indian BPOs to implement the best security practices for handling the data they collect while rendering services.

Section 43A obliges all businesses which handle sensitive personal information to follow "reasonable security practices and procedures". The definition of these in the explanation to section 43A clearly shows that the parties involved are at liberty to identify the best security practices and incorporate them in an agreement. Further, the security practices can be specified either by the central government coupled with the assistance of industry organizations, or by any other law. So far the government has not notified any framework pursuant to the new section, nor is the phrase described elsewhere; accordingly the parties are free to agree mutually acceptable terms regarding security measures, including the applicable law.

There is no cap on the quantum of the penalty that may be imposed in the event of breach under section 43A, meaning that Indian BPO businesses that do not conform to the statutory "reasonable security practices" obligation expose themselves to potentially huge damages claims. It remains to be seen how the judiciary will implement, interpret and quantify claims under this section.

Section 72A addresses issues relating to data sabotage, with penalties including imprisonment for up to three years, fines of up to Rs500,000 (US$10,000) or both. The section requires bad faith intent by the person misusing "personal information" – a broader term than that used in section 43A, where it is qualified by the adjective "sensitive".

Liability of intermediaries: The term "intermediary" is now defined in more detail. It includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes. ITAA has amended section 79, which dealt with the liability of an intermediary for third party content made available or hosted by it. The section now specifies the conditions under which the intermediary will and will not be liable. Although the intermediary is still obligated to exercise due diligence in relation to third party content, the onus of proof has been shifted from the intermediary to the complainant.

In other helpful changes, the ITAA extends the coverage of the IT act to cover most known cyber offences. These include cyber stalking; dishonestly receiving or retaining computers, data, software or mobile devices; identity theft; cheating by impersonation; voyeurism; and cyber-terrorism. To enable proper investigation of cyber offences, sections 67C and 69B oblige intermediaries to preserve prescribed information and data. In addition, the power to investigate cyber offences (including the power to enter public premises, make searches and arrests) has been conferred on police inspectors, a lower ranking officer than was previously empowered to do so. This will improve law enforcement by ensuring that more police officers are available to investigate cyber offences.

There are also problematic changes in the ITAA. All offences punishable with imprisonment of up to three years have been made "bailable"; the accused is entitled to be released on bail as a matter of right, without discretion of the court, risking the possibility of an accused tampering with or destroying evidence upon release. These offences have also been made "non-cognizable", meaning that a police officer has no authority to arrest without a warrant.

As most offences in the IT act are not punishable with imprisonment for over three years, these changes give the law an insufficient deterrent effect. Given India's overburdened courts, convictions are invariably delayed; so, the initial pretrial arrest is important to send the right signal across.

Supporting IT growth while preventing criminals from exploiting weaknesses in IT systems is a daunting task; it is vital to have an effective law that enables investigation and successful prosecution.

Whether the amended IT Act will prove to be effective remains to be seen.

Priti Suri is the proprietor of PSA, where Mahendra Singh chairs the IP practice.