CONTENTS

Recent Amendments in the Information Technology Act, 2000

Recent Amendments in the Information Technology Act, 2000

INTRODUCTION

The Information Technology Act, 2000 **(the "IT Act")** of India has recently undergone a major overhaul, only eight years after it came into force. In December 2008, the long pending amendments to the IT Act were finally passed by the Parliament. Although these amendments are yet to be implemented, they have nevertheless attracted a lot of attention not only for the changes they seek to make in the law but also for the manner and circumstances under which they have been brought. This newsletter gives a historical background of the amendments, discusses the major changes they have introduced, and lastly, attempts to evaluate the amendments themselves.

1. Historical Background

1.1 The IT Act

Based on the UNCITRAL Model Law on E-Commerce, the IT Act came into force on October 17, 2000. It was enacted keeping in mind the technological scenario existing at that time. As technology has the habit of transforming and reinventing itself, it becomes necessary to have a fresh look at any technology-related law from time to time. Over the past few years, amid rising concerns about issues like data security, data privacy, identity theft, hacking, child pornography, cyber terrorism, spam, phishing and other online offences, a need was felt for revising the provisions of the IT Act.

The amendment process that began with the setting up of an expert committee in January 2005 to review the IT Act culminated on February 5, 2009 with the President according her assent to the amendment bill which became the "Information Technology (Amendment) Act, 2008" **(the "ITAA 2008")**. Although ITAA 2008 has not come into force yet pending finalization of the draft rules and issuance of the necessary notification, some of the significant changes introduced by it deserve to be examined.

2 Major Changes Introduced by ITAA 2008

2.1 Data Protection

To satisfy the long-felt need for protecting confidential data and information handled by the Business Process Outsourcing **("BPO")** sector, ITAA 2008 formally introduces the concept of data protection in Indian law and provides for civil and criminal liability for failure to protect personal data and information[1]. Section 43A imposes the obligation to follow reasonable security practices and procedures on all businesses handling sensitive personal data or information. The explanation to section 43A that defines "reasonable security practices and procedures" clearly shows that the parties involved are at liberty to identify the best security practices and incorporate them in a binding agreement. Further, the section also provides that the security practices can be specified either by Government of India 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. Accordingly, the parties are free to agree on mutually

[1] Refer to sections 43A and 72A, newly introduced.

acceptable terms regarding the security measures, including the applicable law. Interestingly, there is no cap on the quantum of the penalty that may be imposed in the event of breach under section 43A. This means that Indian BPO businesses that do not conform to the statutory "reasonable security practices" obligation expose themselves to potential claims for damages that are not capped. Needless to say, it remains to be seen how the judiciary will implement, interpret and quantify claims under this section.

A new section, 72A, addresses issues emerging from data sabotage, and imposes punishment of up to three years or fine up to INR 500,000 (US $ 10,000), and in some cases, both. It is important to note that the section requires *mala fide* intent by the person misusing the information, even as it uses the broader term "personal information" without the prefix "sensitive" used in section 43A. These new sections impose strong legal obligations on Indian BPOs to implement the best security practices for securing data obtained by them while rendering services.

2.2 Liability of Intermediaries

The term "intermediary" has been given a broader definition now and covers telecom/network/internet/webhosting-service providers, search engines, online payment/auction sites, online-market places as well as cyber cafes. Section 79 that dealt with the liability of an intermediary for third party content has been amended for greater clarity and the onus of proving liability has been shifted from the intermediary to the complainant. To enable proper investigation into cyber offences, intermediaries are now obligated to preserve and retain all officially prescribed information for the prescribed duration[2]. They are also required to provide traffic data or information to the prescribed official agency[3]

2.3 More Cyber Offences Covered

To deal with rapidly increasing cyber crime, ITAA 2008 introduces several new offences in the IT Act and also strengthens the existing criminal provisions. To improve law enforcement, the power to investigate offences committed under the IT Act, to enter public premises, to undertake search and to make arrest is now exercisable by a police officer of the rank of an Inspector instead of the higher ranked Deputy Superintendent of Police **("DSP")** earlier.

Section 66 that dealt with hacking has been expanded whereby all the acts of vandalism mentioned in section 43 have been made punishable and the fine has been increased[4].

The new cyber offences added to the IT Act are cyber stalking, spam, threat mails & offensive messages, dishonestly receiving or retaining computer/data/software/mobile devise, identity theft, cheating by impersonation, voyeurism, invasion of privacy and cyber-terrorism[5]. The provisions related to obscenity have been expanded and rationalized by introducing different degrees both of obscenity and punishment, with child pornography attracting the highest punishment.

2.4 National Security

ITAA 2008 attaches great importance to issues involving national security and empowers the Central Government to direct intermediaries to block websites on grounds like defence, state security and public order[6]. Computer systems, networks, data and software whose incapacitation or destruction can prejudice national security, economy, public health or safety have been designated as "*Critical Information Infrastructure*"[7] and any mala fide act adversely affecting it is treated as an act of "cyber terrorism" which term also covers any cyber offence that causes death/injuries, damage to property and disruption of

[2] Refer to section 67C, newly introduced, which also provides for the punishment of imprisonment for up to three years along with fine for intentional or knowing contravention of this requirement.

[3] Refer to section 69B, newly introduced. For intentional or knowing contravention of this requirement, the section provides for the punishment of imprisonment for up to three years along with fine.

[4] From INR 200,000 (US $ 4,000) to INR 500,000 (US $ 10,000)

[5] Refer to newly introduced sections 66A, 66B, 66C, 66D, 66E and 66F respectively.

[6] Refer to section 69A, newly introduced. Blocking is subject to prescribed procedural safeguards. Reasons must be recorded in writing before passing such an order. Contravention of Government's direction is punishable with imprisonment for up to seven years along with fine.

[7] Refer to section 70 that has been amended.

essential services[8]. Provision has been made for the creation of a national nodal agency which shall be responsible for taking all measures to protect critical information infrastructure[9]. Provision has also been made for the creation of the "Indian Computer Emergency Response Team" **("CERT-In")** which is meant to serve as the national agency for preventing and responding to cyber security incidents[10].

2.5 Electronic Signature

As technology changes quite fast, the provisions of the IT Act that involve parameters likely to change from time to time have been amended in such a way as to provide for new developments to be incorporated through the simpler mechanism of delegated legislation. A notable example of this is the introduction of the technologically-neutral concept of "electronic signature" for security, integrity and authentication of electronic records. As and when technology other than digital signature matures, the details of new types of electronic signature will be provided in the rules to be issued by the Central Government, thereby avoiding the need for amending the Act every time.

3 An Evaluation of the Changes

3.1 Some Positives

ITAA 2008 extends the coverage of the IT Act to most known cyber offences. To improve law enforcement, the policing powers have been delegated to a lower rank officer which is expected to ensure availability of more police officers. The liability of intermediaries is now defined more clearly. For proper investigation of cyber offences, intermediaries have been obligated to preserve prescribed information and data. ITAA 2008 also addresses the concerns among foreign businesses regarding outsourcing work to India. The new provisions regarding fixing the liability of Indian BPOs should encourage greater outsourcing to India.

3.2 Some Negatives

All offences that are punishable with imprisonment of up to three years have been made "bailable" which means that the accused is entitled, as a matter of right, to be released on bail. The grant of bail does not depend on the discretion of the court. This creates the possibility of the accused tampering with or destroying evidence upon release. Further, all such offences have been made "non-cognisable" meaning that a police officer has no authority to arrest without warrant. Given the fact that most of the offences in the IT Act do not involve punishment greater than three years, this means that the law would not have as much deterrent effect as it should have. In a country with overburdened courts, convictions are invariably delayed and so, the initial pre-trial arrest is often important to send the right signal across.

3.3 Criticism in Media

ITAA 2008 has attracted criticism on the ground that it was passed by the Parliament hastily without any debate. However, this criticism is not justified given that the amendments were pending since 2005 when an Expert Committee was constituted and have been discussed much since then. There were 17 other bills that were passed by the Parliament on December 23, 2008 within a span of 15 minutes and so it is not fair to single out ITAA 2008!

The amendments have also been criticised for conferring unrestricted powers on government officers, agencies and instrumentalities. It has also been alleged that they violate fundamental rights and civil liberties of citizens. However, looking at the cyber-crime statistics, this criticism does not seem to be justified. The statistics revealed by the National Crime Records Bureau indicate a 50% spurt in cases registered under the IT Act during 2007[11]. According to CERT-In, the number of cyber attacks including viruses, worms and frauds is rising by 15% every year while some are doubling every year. Further, the monthly percentage of personal computers infected by virus in the country has grown from about 1% in 2001 to about 17% in 2007 and the number of

[8] Refer to section 66F, newly introduced, which also provides for life imprisonment for committing an act of cyber terrorism.
[9] Refer to section 70A, newly introduced.
[10] Refer to section 70B, newly introduced.

[11] Available at the web link http://ncrb.nic.in/cii2007/cii-2007/CHAP18.pdf; accessed on August 24, 2009

phishing cases too was rising among Indian banks. In the Mumbai attack of November 2008, terrorists used satellite phones, GPS systems, remailer service and switchable SIM cards to maintain anonymity, showing how sophisticated terrorism has become.

CONCLUSION

For law enforcing agencies, tackling cyber-crimes is emerging as a pressing priority. It is a daunting task to simultaneously ensure IT-enabled growth and at the same time prevent criminals from exploiting weaknesses in IT systems and networks. It is important to have an effective law to enable investigating and prosecuting agencies to bring cyber criminals to book. Whether the IT Act will serve this purpose after the amendments come into force remains to be seen. ***(Mahendra Singh)***

Contact Lawyer

Priti Suri
p.suri@psalegal.com
Mobile + (91) 98100-92842

Mahendra Singh
m.singh@psalegal.com
Mobile + (91) 98183-05946

Contact Details

PSA
Legal Counsellors
E-601, Gauri Sadan
5, Hailey Road
New Delhi – 110 001
India

Tel: + (91 11) 43500-500
Fax: + (91 11) 43500-502