# Legislative Brief

## The Information Technology (Amendment) Bill, 2006

The Bill was introduced in the Lok Sabha on 15th December, 2006 and referred to the Standing Committee on Information Technology (Chairperson: Nikhil Kumar).

The Standing Committee presented its report in Lok Sabha on 7th September, 2007.

**Recent Briefs:**

The Clinical Establishments (Registration and Regulation) Bill, 2007
November 13, 2007

The Private Detective Agencies (Regulation) Bill, 2007
November 2, 2007

**Chakshu Roy**
chakshu@prsindia.org

**November 19, 2007**

### Highlights of the Bill

- The Information Technology (Amendment) Bill, 2006 amends the Information Technology Act, 2000.
- The Bill makes a company handling sensitive personal data liable to pay compensation up to Rs 5 crore, if it is negligent in implementing reasonable security measures with respect to such data.
- The Bill does not hold intermediaries liable for third party data or content made available by them. This protection is not absolute and intermediaries are required to remove unlawful data or content on receiving information about it.
- The Bill proposes to enable authentication of electronic records by any electronic signature technique.
- The Bill changes the name and the composition of the appellate tribunal. It also establishes an examiner of electronic evidence to give expert opinion on "electronic form evidence".

### Key Issues and Analysis

- The Bill enables the central government to intercept computer communication for investigation of any offence. Telephones and letters may be intercepted only to protect national interest, sovereignty etc.
- Neither the IT Act nor any other law covers how personal information may be collected, processed, shared and used. While the Bill provides compensation for unlawful loss or gain arising from unauthorised use of data, it does not address the issue of breach of privacy.
- Any person copying or destroying data without permission of the owner is liable to pay damages. The Bill does not cover situations in which an employee who has permission to access certain data misuses such data.
- Intermediaries are not liable for third party data. They are required to remove unlawful content on receiving "actual knowledge". This term is not defined.
- The expert committee appointed to suggest amendments to the IT Act had recommended stringent punishment for child pornography. The Bill does not address this. The Standing Committee stated that the issue of unwanted commercial e-mails (spam) has not been addressed.

# PART A: HIGHLIGHTS OF THE BILL[1]

## Context

The Information Technology Act, 2000 (IT Act) is based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996.[2] The IT Act provides legal recognition to electronic commerce transactions, allows electronic filing of documents and penalises computer related crimes. The government set up an expert committee to review the IT Act in January 2005. The committee which comprised of representatives from the government, IT industry, legal experts etc. submitted its report in August 2005.[3]

The committee recommended that the IT Act be made technology neutral.• It revisited the provisions related to data protection and privacy and proposed stringent provisions for handling sensitive personal data. The committee addressed the issue of liability of intermediaries and suggested amendments using the European Union Directive on E-Commerce as the guiding principle.[4] It suggested severe punishments to prevent child pornography. It also made recommendations on computer related crime and electronic evidence.

## Key Features

The Information Technology (Amendment) Bill, 2006 proposes to amend the IT Act to (a) make the authentication of electronic record technology neutral,[5] (b) provide for protection of personal information, (c) change the name and constitution of the appellate tribunal, (d) limit the liability of intermediaries and (e) establish an examiner of electronic evidence. It specifies that publishing or transmitting of offensive or pornographic material in electronic form would be an offence. In addition the Bill amends the Indian Penal Code, 1860 to include new offences such as identity theft and recording or transmitting nude images of a person without his permission.

The proposed amendments in the Bill are compared with the existing provisions of the IT Act in Table 1.

**Table 1: Comparison of the Bill with the existing law**

| | Information Technology Act, 2000 | Information Technology (Amendment) Bill, 2006 |
|---|---|---|
| Definition | "Intermediary" means any person who on behalf of another person receives stores, transmits or provides any service with respect to an electronic message. | The Bill adds to the definition of "Intermediary". It specifically includes telecom, network, internet and web hosting service providers, search engines, online payment and auction sites, online market places and cyber cafes in the definition of intermediaries. |
| | | Body corporates handling "sensitive personal data" are excluded from the definition of intermediary. |
| | Cyber Café not defined. | "Cyber Café" means any facility from where internet access is provided to the public in the ordinary course of business. |
| Technology neutral | A person may authenticate an electronic record by a digital signature. Digital signature technology is a form of encryption. | A person may authenticate an electronic record by an electronic signature.* The Bill proposes to substitute the phrase "digital signature" with "electronic signature". This change would make the IT Act technology neutral. |
| Protection of personal information | No Provision. | A body corporate shall be liable to pay compensation if it is negligent in implementing "reasonable security precautions" with respect to "sensitive personal data". The liability would arise if the negligence leads to a wrongful loss or wrongful gain to a person. |
| | | A person is held liable if he discloses "personal information" which he accessed while providing services under a contract. The liability arises if the disclosure was made with an intention to cause or knowing that he is likely to cause wrongful loss or wrongful gain to a person. |
| Liability of intermediaries | An intermediary shall not be responsible for any third party information, data made available by him. | An intermediary shall not be responsible for any third party information, data or communication link made available by him. |
| | To avail of this protection he shall have to prove that data or content which led to the offence was committed without his knowledge or that he exercised due diligence to prevent the commission of such offence. | This protection shall be available if the intermediary only provides access to information and if he does not (a) initiate/ select the receiver of the transmission, and (b) select or modify the information contained in the transmission. The protection is not available if the intermediary conspires or abets in the commission of the unlawful act. Upon receiving actual knowledge or being notified by the government authority about unlawful data or content the intermediary is required to remove such data or content or disable access to it. |

• Technology neutral means neither promoting nor discouraging the use of a particular technology. For example: A law requires that goods need to be transported from one point to another. Requiring the use of trucks to transport goods would make the law technology specific. Specifying that any means of transport may be used to transport goods, such as airplanes, railways, tempos, bullock carts etc., would make the law technology neutral.

* The term "electronic signature" is technology neutral. It describes the full range of technologies that can be used for authenticating an electronic record. It includes digital signature.

| | Information Technology Act, 2000 | Information Technology (Amendment) Bill, 2006 |
|---|---|---|
| Interception and monitoring of information | The power of interception is vested with the Controller of Certifying Authorities.<br>He may intercept any information transmitted through any computer resource in the interest of national security, sovereignty, public order etc. | The power of interception is now vested with the central government.<br>In addition to the existing circumstances under the IT Act, the central government may intercept /monitor any information transmitted through any computer resource for investigation of any offence. |
| New offences | | The Bill adds eight new offences: five under the IT Act and three under the Indian Penal Code, 1860.<br>Offences under the IT Act include, sending offensive messages through a computer or mobile phone, publishing or transmitting material in electronic form containing sexually explicit act, disclosing information in breach of lawful contract.<br>Under the Indian Penal Code punishment is provided for identity theft, cheating by personation using computer resource and for recording or transmitting nude images of a person without his permission. |
| Change in penalties | More imprisonment, lower fines. | Less imprisonment, higher fines. |
| Electronic document filing with government | No provision. | The government may authorise any service provider to provide electronic document filing services to the public for a fee. |
| Formation and validity of contracts | No provision. | Contracts formed through electronic means shall not be unenforceable solely on the ground that the contract was entered into electronically. |
| Examiner of electronic evidence | No provision. | To give expert opinion on "electronic form evidence" before any court/authority the central government may appoint an "examiner of electronic evidence". |
| Appellate Tribunal | The appellate authority under the IT Act is called the "Cyber Regulations Appellate Tribunal". It consists of only one person to be appointed by the government. | The name of the appellate tribunal is changed to, "Cyber Appellate Tribunal". It would consist of a chairperson and other members to be appointed by the government. One member of the tribunal would be a judicial member. |

Sources: Information Technology Act, 2000; Information Technology (Amendment) Bill, 2006; PRS

# PART B: KEY ISSUES AND ANALYSIS

## Interception of Messages

Clause 33

In India letters, postal articles, phones, emails and computer messages can be intercepted by the government in the interest of national security, sovereignty, public order etc. The Bill expands the power of the central government to include interception of information transmitted through a computer resource for the purpose of investigation of any offence. Table 2 compares the power of the government to intercept messages sent through different mediums.

**Table 2: Comparison of power of the government to intercept messages**

| Type of Message | Condition for interception | Law applicable |
|---|---|---|
| Letter/postal articles | On the occurrence of any public emergency; or in the interest of public safety or tranquillity | Sec 26, The Indian Post Office Act, 1898 |
| Land line / mobile phones | On the occurrence of any public emergency; in the interest of public safety; sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; or for preventing incitement to the commission of an offence | Sec 5(2), The Indian Telegraph Act, 1885 |
| Email / Computer messages (Existing law) | Sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; or for preventing incitement to the commission of a cognizablen offence | Sec 69, IT Act |
| Email / Computer messages (Proposed) | Investigation of any offence | Clause 33, IT Amendment Bill |

Sources: The Indian Post Office Act, 1898; The Indian Telegraph Act, 1885; PRS

The Standing Committee on Information Technology, while reviewing the Bill, observed that "Public Order" and "Police" are state subjects as per Schedule VII of the Constitution. It was of the view that it would be appropriate and expedient to confer powers of interception on the State Governments in tune with the provisions of Section 5(2) of the Indian Telegraph Act, 1885. It also recommended that interception should be allowed for prevention of any cognizable offence• in addition to the already prescribed grounds.

• A cognizable offence (listed in the First Schedule to the Code of Criminal Procedure, 1973) is one in which a police officer may arrest a person without a warrant.

## Data Protection

Clauses 20, 36

The European Union defines data protection as securing for every individual, respect for his rights and fundamental freedoms and in particular his right to privacy, with regard to automatic processing of personal data relating to him.[6] Separate legislation for data protection exists in many countries.[7] India does not have specific legislation for data protection. The IT Act is a law to facilitate e-commerce and has some provisions for protecting data.

Lack of separate legislation for data protection implies that individuals have no control over how their personal data is collected, processed and used. Thus under the amended Act, companies are not prohibited from selling or sharing their customers personal data with telemarketers or recovery agents. Also the protection of data as proposed in the Bill is only against wrongful loss or wrongful gain and not against breach of privacy.

The Standing Committee observed that, there is no specific provision in the Bill for protection and retention of data. The Committee also observed that suitable provisions to define and protect personal privacy should be added.

### Definitions

Clauses 20, 36

The Bill proposes to add two more provisions to protect data in addition to existing provisions. The first provision protects "sensitive personal data" and the second protects "personal information".[8] The Bill requires the central government to define "sensitive personal data". "Personal information" is not defined.

In the United Kingdom "sensitive personal data" consists of information as to the racial or ethnic origin of a person, his political opinions, religious beliefs, physical or mental health, commission of an offence etc. "Personal data" means data which relates to a living individual who can be identified from such data.[9]

### Liability of Intermediaries

Clause 38

The Bill follows the European Union's E-Commerce Directive to determine the extent of responsibility of intermediaries for third party data or content. As per the Bill intermediaries are not ordinarily responsible for third party content. However this protection is not available if the intermediary, upon receiving actual knowledge or on being notified about unlawful content, fails to quickly remove access to such data or content.

The Bill does not specify as to what constitutes actual knowledge. This could lead to intermediaries stopping access to data/content on receiving frivolous complaints without verifying their genuineness. At the other extreme it could also result in intermediaries requiring a detailed notice before they remove or disable access to content. The Bill also does not protect intermediaries from legal action if they, in good faith, remove data or content to prevent possible unlawful activity. The Bill also does not provide a mechanism for restoring access to data if false complaints are registered with them with respect to data/content.

In the United States, responsibility of intermediaries with respect to copyrighted content is regulated under the Digital Millennium Copyright Act, 1998. It establishes procedures for providing proper notice of unlawful data or content. It also specifies the time frame (10 to 14 days) in which access to data/content would be restored by an intermediary on receiving a counter notice from the data owner that the data is not unlawful. It also requires intermediaries to designate a person to receive notices about data/content. Actions of intermediaries taken in good faith are also protected.

### Misuse of Access to Data

Clause 19

The IT Act makes a person liable to pay damages for copying, downloading or damaging data without permission of the owner. It does not cover situations where a person who has permission of the owner to do certain acts exceeds his mandate. For example an employee may be permitted to access customer data, but could misuse such data. The expert committee constituted to review the IT Act had made a recommendation to prevent such misuse. This has not been incorporated in the Bill.

## Child Pornography

The expert committee constituted to review the IT Act had recommended penalizing publication or transmission of child pornography through electronic form. This recommendation of the expert committee has not been incorporated in the Bill. The Standing Committee in its report observed that specific provisions should be incorporated to criminalise child pornography in tune with laws prevailing in advanced countries and Article 9 of the Council of Europe Convention on Cyber Crime.

## Spam

Clause 31

The Bill makes sending of content which is grossly offensive or of a menacing character through a computer or mobile phone a punishable offence. The Standing Committee observed that the Bill does not adequately address the issue of unwanted commercial e-mails (spam).

## Issues raised by the Standing Committee

The Standing Committee made several recommendations/ observations.

**Table 3: Some recommendations/ observations of the Standing Committee**

| Topic | Standing Committee recommendations/observations |
|---|---|
| Cyber terrorism | Cyber terrorism has not been defined anywhere in the IT Act or in the Bill. Cyber terrorism is equivalent to waging war against the State. Stringent provisions should be incorporated in the IT Act to deal with such offences. |
| Jurisdiction of law | The provisions of the IT Act seem to be inadequate for enforcing the will of the State in cases where cyber crime committed against India from outside India. |
| | India should be a signatory to an international convention on the issue of cross border cyber crime so that such crimes are tackled with promptly. India should take initiative in materialising such an international convention. |
| Technology neutral | Awareness should be created to educate people on the possible misuse/ abuse of digital signatures. Government should make digital records available to the public in people friendly and easily accessible formats. |
| Definition and liability of intermediaries | The definition of an "intermediary" is not very clear particularly in regard to the exclusion of a body corporate which deals with "sensitive personal data". |
| | A definite obligation should be cast upon the intermediaries in view of the damage caused to victims through reckless activities that are undertaken in the cyber space by using the intermediary's platform. |
| | The absence of due diligence to be exercised by the intermediaries like online market places/ auction sites, with respect to third party data or content would disturb the equilibrium with similar entities in the offline world. Due diligence to be exercised by intermediaries should be made a pre-requisite before giving immunity to intermediaries online market places and online auction sites. |
| Compensation for failure to protect sensitive personal data | The government should simplify the complicated adjudication process to ensure that the remedy of providing damages by way of compensation is effectively implemented. |
| Powers of civil courts | Circumstances under which the civil courts role come into play should be spelt out clearly and it should be clarified whether the civil court can restrict the jurisdiction of the appellate tribunal. |
| Training | The government in tandem with the industry should take some measures to initiate some basic training programs for all those dealing with cyber cases. |

Sources: Standing Committee Report; PRS

## International Comparison

Some of the issues related to the Bill as well as those raised by the Standing Committee are addressed by other countries in different ways. The corresponding provisions in the laws of the United States and the United Kingdom are summarised in Table 4.

**Table 4: Some related provisions in the US and UK**

| Topic | United States | United Kingdom | India |
|---|---|---|---|
| Interception | Requires a court order for investigation or prevention of a crime. The long list of offences include those related to chemical weapons and terrorism. | Can be ordered by the government in the interests of national security or for the purpose of preventing / detecting serious crime or for safeguarding the economic well-being of the country. | Can be ordered by the government in the interest of national security, sovereignty and integrity of India etc. This Bill extends this to investigation of any offence. |
| Child pornography | Distribution, reproduction and possession with intent to sell are punishable with up to 15 years imprisonment. | Possession is punishable with maximum of five years imprisonment. Making an indecent image of a child carries a maximum sentence of 10 years imprisonment. | No specific provision. |
| Spam | Sending spam is illegal and punishable with one to five years imprisonment. | The European Union directive on Privacy and Electronic Communication prohibits the sending of spam. | No law on spam. |
| Cyber Terrorism | Damaging protected computers or computers used for national security or criminal justice is punishable with a maximum imprisonment of 20 years. | Collecting information of a kind likely to be useful to a person committing / preparing an act of terrorism is punishable with a term not exceeding 10 years. | No specific provisions to address cyber terrorism. |

Sources: Various Acts[10]; PRS

**Notes**

1. This Brief has been written on the basis of the Information Technology (Amendment) Bill, 2006 introduced in the Lok Sabha on December 15, 2006. The Parliamentary Standing Committee on Information Technology (Chairperson: Nikhil Kumar) submitted its report on September 7, 2007.

2. The model law was adopted by the General Assembly of the UN vide resolution A/RES/51/162, dated January 30, 1997.

3. Press release dated August 29, 2005 issued by the Department of Information Technology, Ministry of Communications & Information Technology. http://www.mit.gov.in/download/PressRelease.doc.

4. European Union Directive 2000/31/EC 8 June 2000.

5. This change is based on the Model Law on Electronic Signatures, it was adopted by UNCITRAL on July 5, 2001.

6. The Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, January 28, 1981.

7. United Kingdom enacted its Data Protection Act in 1984. Countries in the European Union have data protection legislation based on Directive 95/46/EC of the European Parliament. United States of America has sector specific data protection legislation with respect to online privacy of children (Children's Online Privacy Protection Act) and health records of individuals (Health Insurance Portability and Accountability Act).

8. Clause 20 and Clause 36 of this Bill.

9. Section 1(1) and Section 2, Data Protection Act 1998 of United Kingdom.

10. United States: The Omnibus Crime Control and Safe Street Act, 1968, The Child Pornography Protection Act, 1996, Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001. United Kingdom: The Regulation of Investigatory Powers Act, 2000, The Protection of Children Act, 1978, The Criminal Justice Act, Terrorism Act 2000. European Union: European Union Directive 2002/58/EC on Privacy and Electronic Communication.