

Curbing Cyber Crime:
A Critique of
Information technology Act 2000 and IT Act
Amendment 2008

By

Sanjay Pandey
iSec Services Pvt Ltd
608, Reliable Pride, Anand Nagar, Jogeshwari West,
Mumbai-53

Abstract

In the present decade if India made news internationally, in technology sectors, it has been mainly for the contracts that it grabbed for performing data processing activities from offshore. Initially this started with simple transcription centers where voice recorded details were converted into digital data. But lately, this has transformed into knowledge processing centers where complete research is done on various domains which include medicine, law, technology and even media.

Even within the country there has been increasing use of computers. Be it Airline or train reservation system or the initiative towards online collection of direct and indirect taxes, there is great amount of data about individuals and businesses which is available in digital format.

One of the main concerns regarding the existence and use of data on computers has been lack of adequate security legislation in the country. In year 2000 India did enact IT Act and made first attempt at trying to define use and misuse of digital medium in the country.

Analyzing the provisions of IT Act, 2000 and its recent amendments towards combating cyber crime is the basic theme of this paper. While attempting to do this it first analyses the current trends in cyber crime and its ramifications. Second it analyses the needs of legislation and current provisions in the IT Act. Third, this paper discusses similar provisions elsewhere in the world and attempts to draw parallels in existing laws within the country. Finally it sums up the current provisions with suggested recommendations for a possible safe and secure cyber world.

Introduction

The Background

United Nations Commission on International Trade Law in 1996 framed Model Law on Electronic Commerce¹. The United Nations General Assembly by resolution A/RES/51/162, dated the 30 January 1997 adopted this Model law.

This resolution recommended that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

The Ministry of Commerce Government of India created the first draft of the legislation following these guidelines termed as "E Commerce Act 1998". Since later a separate ministry for Information technology came into being, the draft was taken over by the new ministry which re-drafted the legislation as "Information Technology Bill 1999". This draft was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on June 9, 2000, the act was finally notified with effect from October 17, 2000 vide notification number G.S.R 788(E).

Pronouncement passing the legislation also clearly indicated the emphasis behind passing the act-

' An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of

¹ http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.'

Clearly, most sections addressed the need of issuance of digital certificates and management of these certificates. Cyber crime as a subject was not looked into at depth. There were only passing references to acts of cyber crime without mentioning the crime specifically. Therefore since the Act was passed there had been increasing demand to address increasing events of cyber crime.

Chronology of Events

Ever since the Act came into being there were series of demands for bringing about changes that will make sure that the Act provided for curbing the menace of cyber crime. Issues of data leakage and personal privacy also started making news. These demands for change were further strengthened by the BPO industry in India which had to produce credentials of data safety and privacy in India to bid for international projects which were being outsourced out of western countries.

A major amendment was made to the Act with effect from 6 February 2003 consequent to the passage of a related legislation called Negotiable Instruments Amendment Act 2002. The amendment to Negotiable Instruments Act, 2002 for the first time recognized a cheque in electronic form². These changes notwithstanding, Indian government realizing the changing terrain of online interactions, formed an expert committee under Ministry of IT to suggest amendments to act to keep it relevant. Main reasons for looking into changes in the Act were

² <http://www.netlawman.co.in/acts/negotiable-instruments-act-2002.php>

(a) subject matter being information technology which has a accelerated pace of development

(b) intensive approach employed in it as opposed to a general framework to regulate information technology

The committee pointing out several lacuna's in the enactment proposed amendments to it in the report it tendered to the ministry of information technology. The result was the Information Technology Amendment Bill, 2006³ based on the report submitted by the expert committee⁴.

During the same time in order to provide for protection of data leakage and personal privacy a Personal Data Protection Bill was introduced in Rajya Sabha in 2006⁵. This bill, however, remains to be passed. The Information technology Act 2000 amendment Bill 2006⁶ has since been passed by the Indian Parliament on December 23, 2008.

IT Act provisions and Amendments

IT Act 2000

As has been discussed earlier the IT Act 2000 was mainly to ensure legal recognition of e commerce within India. Due to this most provisions are mainly concerned with establishing digital certification processes within the country. Cyber crime as a term was not defined in the act. It only delved with few instances of computer related crime. These acts as defined in Chapter XI of the Act are

³ <http://iltb.apargupta.com/?p=27>

⁴ Expert committee report [http://72.14.235.132/search?q=cache:SxMScP-tN4MJ:www.mit.gov.in/download/ITAct.doc+IT+Act+200&cd=5&hl=en&ct=clnk&gl=in&client=firefox-](http://72.14.235.132/search?q=cache:SxMScP-tN4MJ:www.mit.gov.in/download/ITAct.doc+IT+Act+200&cd=5&hl=en&ct=clnk&gl=in&client=firefox-a)

⁵ http://rajyasabha.nic.in/bills-ls-rs/2006/XCI_2006.pdf

⁶ http://www.prsindia.org/docs/bills/1192012012/1192012012_96_2006.pdf

- a. Illegal access, introduction of virus, denial of services, causing damage and manipulating computer accounts (Section 43)
- b. Tampering, destroying and concealing computer code (Section 65)
- c. Acts of hacking leading to wrongful loss or damage (Section 66)
- d. Acts related to publishing, transmission or causing Publication of obscene/ lascivious in nature (section 67)

Act of causing denial of service, introduction of virus etc as defined in section 43 only amounts to payment of damages which could be upto one crore.

Punishment in section 65 and 66 is three years or fine up to two lakh rupees or both. For section 67 the first time offenders can be punished up to 5 years with fine up to one lakhs of rupees. Subsequent offence can lead to ten years of punishment and fine up to two lakhs of rupees.

IT Act Amendment 2008

IT Act Amendment which came into force after Presidential assent in Feb 2009 has following salient features

Liability of body corporate towards Sensitive Personal Data

New amendment was brought in changes in section 43 of IT Act 2000 in which for the first time any body corporate which deals with sensitive personal information does not have adequate controls resulting in wrongful loss or wrongful gain to any person is liable to pay damages to that person to the tune of five crores.

Introduction of virus, manipulating accounts, denial of services etc made punishable

Section 66 has been amended to include offences punishable as per section 43 which has also been amended to include offences as listed above; punishment may lead to imprisonment which may extend to three years or with fine which may extend to five lakh rupees or with both. This is a change from earlier position where introduction of virus, manipulating some ones account has been made punishable with imprisonment for the first time.

Phishing and Spam

While this has not been mentioned specifically but this can be interpreted in the provisions mentioned here in section 66 A. Through this section sending of menacing, annoying messages and also misleading information about the origin of the message has become punishable with imprisonment up to three years and fine

Stolen Computer resource or communication device

Newly added Section 66B has been introduced to tackle with acts of dishonestly receiving and retaining any stolen computer resource. This has also been made punishable with three years or fine of one lakh rupees or both.

Misuse of Digital Signature

Section 66C. Dishonest use of somebody else's digital signature has been made punishable with imprisonment which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

Cheating

Cheating using computer resource has been made punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee (section 66D)

Cyber terrorism

The newly introduced section 66F talks about acts of cyber terror which threatens the unity, integrity or sovereignty of India or strike terror in the people or any section of the people include

- a. Denial of service of resources in use by nation
- b. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access
- c. Introducing or causing to introduce any computer contaminant likely to cause death or injuries to person or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or
- d. knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the

advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

These acts have been made punishable with Imprisonment which may extend to imprisonment for life

Child Pornography

Newly introduced section 67 B attempts to address the issue of child pornography. Through this section it has made the publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, any one who creates, facilitates or records these acts and images punishable with imprisonment of five years and fine which may extend up to ten lakhs in first offence and seven years and fine of ten lakhs on subsequent offence

Intermediary's liability

Intermediaries have been made liable to retain any information in the format that Central government prescribes. (Sections 67C) and are punishable for violation with a punishment of imprisonment of 3 years and fine

In case of any act which affects national sovereignty intermediaries are liable to seven years (Section 69(4))

Surveillance, Interception and Monitoring

In order to combat cyber terrorism the government has further armed itself with drastic powers Sections 69 of IT Act 2000 amended enhances the scope from the 2000 version to include interception and monitoring.

This has been a major change in the section which also empowers government not only to monitor any traffic but also block any site through any intermediary. Any failure on part of the intermediary is punishable by seven years and also fine (Section 69(4)). Earlier the provision did not mention any fine.

Cognizance of cases

All cases which entail punishment of three years or more have been made cognizable. Offences with three years punishment have also been made bailable (Section 77B). This change though welcome will make sure most cases falling under IT Act will be bailable with sole exception of Cyber terrorism cases, cases related to child pornography and violations by intermediaries in some cases.

Investigation of Offences

One major change has been inclusion of Inspectors as investigating officers for offences defined in this act (section 78). Earlier these investigations were being done only by an officer of the rank of Deputy Superintendent of Police which was a serious limitation mainly because number of officers in this rank is limited. With this change one can look forward to more cases being filed and investigated by police.

Major Dilutions

Sexually explicit content

Newly introduced section 66 E talks about acts of intentionally or knowingly captures, publishes or transmits the image of a private area of any person

without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. In fact the earlier section 67 of IT Act did mention

'any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave..'

and was punishable for first offence with five years of imprisonment and fine of one lakh rupees. This change has made the provision lenient and open to misinterpretation.

Compliance with orders of Controller

Section 68(2) which earlier made failure to comply with the direction of controller punishable with three years of imprisonment or fine of two lacks or both now has been reduced to two years punishment or fine of one lakh of rupees or both

International Scenario

Anti Spam Laws

United States

United States has a specific CAN-Spam Act 2003⁷ which came into force in January 2004. Major provisions are

- False and misleading header information is banned
- Deceptive subject lines are prohibited
- Opt-out methods must be provided
- Commercial email must be identified as an advertisement and it must include the sender's valid physical postal address

⁷

Spam Laws: <http://www.spamlaws.com/spam-laws.html>

- Receivers must be warned of sexually explicit material

Penalties include fine upto USD 11000 and also imprisonment in specific circumstances.

Europe

Europe union through directive on privacy and electronic communication, 2003⁸ has been major driving force behind enactments of anti spam laws in Europe. Uk imposes a fine of GBP 5000 on spammers if they fall within the ambit of its Anti Spam Act.

Computer Misuse

United States

This was addressed in US way back in 1984 through **Computer Fraud and Abuse Act**⁹. This act governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce¹⁰. This act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so. This act has been further amended by **US Patriot Act, 2001** which enhanced the scope and penalties imposed. First offence penalties are ten years imprisonment and second offence penalty is imprisonment of 20 years. These are much more stringent considering Indian law provides for just around three years punishment in most cases.

UK

⁸ European Union directive: <http://www.opsi.gov.uk/si/si2003/20032426.htm>

⁹ Computer Fraud and Abuse Act, 1984 USA:

<http://72.14.235.132/search?q=cache:GmkLMLpO3jgJ:cio.energy.gov/ComputerFraud-AbuseAct.pdf+computer+fraud+and+abuse+act&cd=4&hl=en&ct=clnk&gl=in&client=firefox-a>

¹⁰ Compute fraud and abuse act: http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

UK computer misuse was defined in 1990 through its **Computer Misuse Act**¹¹ . This act dealt with unauthorized access, modification of computer material. Penalties imposed are to the tune of five years imprisonment with fine.

Data Protection and Personal Privacy

These have been of major concern internationally and legislations have been passed as long ago as 1998 to ensure protection of personal data. One of the leading legislations is the **Data Protection Act, 1998 of UK**. This act specifically defines sensitive personal data as

“In this Act “sensitive personal data” means personal data consisting of information as to—

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.”

While Indian IT act Amendment talks about ‘sensitive personal data’ in section 43 but fails to define what exactly it implies by sensitive personal data.

¹¹ Computer Misuse Act, UK: http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm

USA

Identity Theft Enforcement and Restitution Act of US has made further enhancements to the original act (Computer Fraud and Abuse Act, 1984) by making the act of causing damage to ten or more computers as felony. It also removed the limit of damage which was earlier set to USD 5000 in Computer Fraud and Abuse Act. One of the major emphasis of this act has been to criminalize not only explicit threats to cause damage to a computer, but also threats (1) to steal data on a victim's computer, (2) to publicly disclose stolen data, or (3) to not repair damage the offender already caused to the computer; and also ensuring that restitution orders for identity theft cases may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated identity theft offense

Conclusion

Indian IT act Amendment though has made a major attempt to address issues related to cyber crime, it still falls short on many counts. Some of the major shortcoming which we feel need to be addressed are

Pornography

Section 67 of the IT Act lays down the law that obscenity is an offence when it is published or transmitted or caused to be published in any electronic form. The expressions, 'publishing' or 'transmission' have not been specifically defined under the IT Act.

Data Protection

The Information Technology Act talks about unauthorized access in section 43 of the IT Act but it does not talk about maintaining integrity of customer transactions. U.K has a data protection law which was enacted 10 years back

that is in 1998¹² under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data.

US

Spamming

Spamming is a growing menace and India figures in top 10 countries as originators of spam. Still this has not been addressed in the manner it should be considering the wastage it causes. One may argue that section 43 of IT Act¹³ while referring to

“(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; “ deals with spam. This however leaves a lot to interpretation.

Identity Theft

Identity theft worldwide is a growing problem. IT act 2000 fails to address this issue. This is a major drawback considering the fact that majority of outsourcing work that India does requires the companies in India to ensure there is no identity theft. In fact identity theft was one of the main reasons for

¹² Data Protection Act 1998, UK : http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

¹³ IT Act : <http://www.legalserviceindia.com/cyber/itact.html>

a major hue and cry over an incident involving personal information of UK customers and an Indian web marketing company¹⁴.

As country develops into a more robust economy and use of computers becomes ubiquitous, it is imperative that our laws are updated to respond to changing scenario. Quite unlike other penal laws IT Act in particular needs revision and reviews much more regularly mainly due to rapid changes in use of Information Technology.

¹⁴ Horror of outsourcing to India - Indian call centers are illegally selling personal information of tens of thousand Australian customers <http://www.indiadaily.com/editorial/4198.asp>