50

STANDING COMMITTEE ON
INFORMATION TECHNOLOGY
(2007-2008)

FOURTEENTH LOK SABHA

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(DEPARTMENT OF INFORMATION TECHNOLOGY)

INFORMATION TECHNOLOGY (AMENDMENT) BILL, 2006

FIFTIETH REPORT

LOK SABHA SECRETARIAT
NEW DELHI

AUGUST, 2007/BHADRAPADA, 1929 (Saka)

FIFTIETH REPORT

STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2007-2008)

(FOURTEENTH LOK SABHA)

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DEPARTMENT OF INFORMATION TECHNOLOGY)

INFORMATION TECHNOLOGY (AMENDMENT) BILL, 2006

Presented to Lok Sabha on 7.9.2007
Laid in Rajya Sabha on 7.9.2007

LOK SABHA SECRETARIAT
NEW DELHI

AUGUST, 2007/BHADRAPADA, 1929 (Saka)

CONTENTS

COMPOSITION OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2007-2008)

Shri Nikhil Kumar - ***Chairman***

Lok Sabha

2. *Shri Abdullakutty*
3. *Shri Ramesh Dube*
4. *Shri Nikhil Kumar Choudhary*
5. *Shri Sanjay Shamrao Dhotre*
6. *Smt. Jayaprada*
7. *Shri Narahari Mahato*
8. *Shri Bhubaneshwar Prasad Mehta*
9. *Shri Harish Nagpal*
10. *Shri G. Nizamuddin*
11. *Shri Sohan Potai*
12. *Shri Lalmani Prasad*
13. *Kunwar Jitin Prasad*
14. *Shri Badiga Ramakrishna*
15. *Shri Vishnu Deo Sai*
16. *Shri Tufani Saroj*
17. *Shri Tathagata Satpathy*
18. *Smt. Rubab Sayeda*
19. *Shri K.V. Thangka Balu*
20. *Shri P.C. Thomas*
21. *Shri Kinjarapu Yerrannaidu*

Rajya Sabha

22. *Shri Praveen Rashtrapal*
23. *Shri Ravi Shankar Prasad*
24. *Shri Dara Singh*
25. *Shri A. Vijayaraghavan*
26. *Shri N.R. Govindrajar*
27. *Shri Motiur Rahman*
28. *Shri Eknath K. Thakur*
29. *Shri Shyam Benegal*
30. *Shri Rajeev Chandrasekhar*
31. *Shri Gireesh Kumar Sanghi**

SECRETARIAT

1.	Shri Rajagopalan M. Nair	-	Additional Secretary
2.	Shri P.Sreedharan	-	Joint Secretary
3.	Shri P.C. Koul	-	Deputy Secretary
4.	Shri D.R. Mohanty	-	Under Secretary

* Nominated with effect from 24th August, 2007.

INTRODUCTION

I, the Chairman, Standing Committee on Information Technology (2007-08) present this Fiftieth Report on 'Information Technology (Amendment) Bill, 2006' relating to the Ministry of Communications and Information Technology (Department of Information Technology).

2. The Information Technology (Amendment) Bill, 2006 was introduced in Parliament on 15th December, 2006 and referred to this Committee on 19th December, 2006 for examination and report within three months. However, due to other pressing assignments and the wide range of consultations/interactions required for and in connection with the examination of this vital piece of legislation, the Committee sought extension of time to finalise their Report. Speaker, Lok Sabha was pleased to accord extension of time upto the end of the Monsoon Session to present the Report to the House.

3. In the process of the examination of the Bill, the Committee received extensive inputs in the form of several write-ups/suggestions from the stakeholders/industry/legal luminaries/NGOs/general public and heard their views at the sittings of the Committee held on 20th April, 2007, 8th May, 2007, 21st May, 2007 and 22nd May, 2007. The Committee received inputs also from the Central Bureau of Investigation (CBI) and the Ministry of Law & Justice (Legislative Department). The representatives of the Legislative Department tendered evidence before the Committee on 14th May, 2007 and 11th June, 2007 and those of CBI on 11th June, 2007. Besides furnishing background material, written replies and several clarifications, the representatives of the Department of Information Technology deposed before the Committee on 29th January, 2007, 22nd February, 2007, 16th July, 2007 and 23rd July, 2007.

4. The Draft Report was considered and adopted by the Committee at their sitting held on 29th August, 2007.

5. The Committee wish to express their thanks to Shri Pavan Duggal, Senior Advocate, Supreme Court, Shri P.K.H. Tharakan, Secretary (Retd), R&AW, Smt. Vidya Reddy as well as the representatives of National Association of Software & Service Companies (NASSCOM), Federation of Indian Chambers of Commerce & Industry (FICCI) and Associated Chambers of Commerce (ASSOCHAM) for appearing before the Committee and furnishing written inputs/suggestions on the amending Bill.

6. The Committee also wish to express their thanks to the representatives of the Central Bureau of Investigation (CBI), Legislative Department and the Department of Information Technology for tendering evidence before the Committee and providing valuable information/clarifications that the Committee desired in connection with examination of the Bill.

7. Last but not the least, the Committee would like to place on record their deep appreciation of the huge amount of spadework done by their predecessor Committee (2006-07) for and in connection with the examination of the Amending Bill. The Committee benefited substantially from the untiring efforts and the hard work done by their predecessor Committee.

8. For facilitation of reference and convenience, the observations and recommendations of the Committee have been printed in bold in the body of the Report.

New Delhi

31st August, 2007
09 Bhadrapada, 1929 (Saka)

NIKHIL KUMAR

CHAIRMAN
STANDING COMMITTEE ON INFORMATION TECHNOLOGY

REPORT

Introductory

The Information Technology Act was enacted in the year 2000 and implemented w.e.f 17th October, 2000 to give a fillip to the growth and usage of computers, internet and software in the country as well as to provide a legal framework for the promotion of e-commerce and e-transactions in the country. The Information Technology Act, 2000 which consist of 94 Sections in 13 Chapters and with Four Schedules provides for a legal framework for evidentiary value of electronic record and computer crimes which are of technological nature.

2. The salient features of the Information Technology Act, 2000 are as follows:-

i) Extends to the whole of India (Section 1)
ii) Authentication of electronic records (Section 3)
iii) Legal Framework for affixing Digital signature by use of asymmetric crypto system and hash function (Section 3)
iv) Legal recognition of electronic records (Section 4)
v) Legal recognition of digital signatures (Section 5)
vi) Retention of electronic record (Section 7)
vii) Publication of Official Gazette in electronic form (Section 8)
viii) Security procedure for electronic records and digital signature (Section 14, 15, 16)
ix) Licensing and Regulation of Certifying authorities for issuing digital signature certificates (Section 17-42)
x) Functions of Controller (Section 18)
xi) Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities (Section 19)
xii) Controller to act as repository of all digital signature certificates (Section 20)
xiii) Data Protection (Section 43 & 66)
xiv) Various types of computer crimes defined and stringent penalties provided under the Act (Section 43 and Section 66, 67, 72)
xv) Appointment of Adjudicating officer for holding inquiries under the Act (Section 46 & 47)
xvi) Establishment of Cyber Appellate Tribunal under the Act (Section 48-56)

xvii) Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court (Section 57)

xviii) Appeal from order of Cyber Appellate Tribunal to High Court (Section 62)

xix) Interception of information from computer to computer (Section 69)

xx) Protection System (Section 70)

xxi) Act to apply for offences or contraventions committed outside India (Section 75)

xxii) Network service providers not to be liable in certain cases (Section 79)

xxiii) Power of police officers and other officers to enter into any public place and search and arrest without warrant (Section 80)

xxiv) Offences by the Companies (Section 85)

xxv) Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (Section 88)

3. The computer crimes in the Act are classified into two categories i.e. civil penalties and criminal offences, the details of which are as follows:-

Civil-Penalties	Section	Criminal offences	Section
• Unauthorised access	43 (a)	• Tampering with computer source documents (i.e. listing of programmes)	65
• Unauthorised copying, downloading and extraction of files	43 (b)	• Hacking computer system	66(1)
• Introduction of virus	43 (c)	• Electronic forgery i.e. affixing of false digital signature, making false electronic record	74
• Damage to Computer System and computer Network	43 (d)	• Electronic forgery for the purpose of cheating	74
• Disruption of computer, computer network	43 (e)	• Electronic forgery for the purpose of harming reputation	74
• Denying authorised person access to computer	43 (f)	• Using as genuine a forged electronic record	
• Providing assistance to any person to facilitate unauthorized access to a computer	43 (g)	• Publication for fraudulent purpose	
• Charging the service availed by a person to an account of another person by tampering and manipulation of other computer	43 (h)	• Offences and contravention by companies	85
• Failure to furnish information, return, etc. to the Controller or Certifying Authority	44	• Unauthorised access to protected system	70
		• Confiscation of computer, network, etc.	76
		• Publication of information which is obscene in electronic form	67

		• Misrepresentation or suppressing of material fact while obtaining any licence or digital signature	71
		• Breach of confidentiality and Privacy	72
		• Publishing fake Digital Signature Certificate	73

4. The following are excluded from the purview of the Information Technology Act, 2000:-

i) Power of Attorney
ii) Trust
iii) Will, and
iv) Any contract for the sale or the conveyance of immovable property or any interest in such property.

5. Through the Information Technology Act, amendments have been made in the following other Acts:-

(i) Indian Evidence Act, 1872
(Sections 3, 17, 22, 34, 35, 39, 47, 59, 65, 67, 73, 81, 85, 88, 90 & 131)

(ii) Indian Penal Code, 1860
(Sections 29, 167, 172, 173, 175, 192, 204, 463, 464, 466, 468, 469, 470, 471, 474, 476, & 477)

(iii) Bankers Book Evidence Act, 1891
(Section 2)

(iv) Reserve Bank of India Act, 1934
[Section 58 (Sub Section (2) Clause (P)]

6. The Information Technology Act, 2000 was enacted keeping in view technology directions and scenario as it existed at that point of time. As the technology has a habit of reinventing itself into cheaper and more cost effective options, it becomes imperative to give a fresh look to any technology driven law from time to time. Moreover, due to overall increase in e-commerce, growth in outsourcing business, new forms of transactions, new means of identification, consumers concern, promotion of e-governance and other information

technology applications, technology neutrality from its present 'technology specific' form in consonance with development all over the world, security practices and procedures for protection of Critical Information infrastructure, emergence of new forms of computer misuse like child pornography, video voyeurism, identity theft and e-commerce frauds like phishing and online theft, rationalization of punishment in respect of offences with reference to the Indian Penal code, a need was felt to review the Indian Information Technology Act, 2000.

7. In that direction, an Expert Committee was set up in January, 2005 under the Chairmanship of the Secretary, Department of Information Technology. The Expert Committee comprised various representatives of the Government, legal experts in the areas of Cyber Laws, Service Providers, representatives of IT Industry and apex industry Associations, National Association for Software Companies (NASSCOM) and Manufacturers Association of Information Technology (MAIT). The mandate of the Expert Committee was to review the provisions of the IT Act, 2000, to consider the feasibility of making the Act technology neutral and recommend necessary amendments to that effect, and to recommend suitable legislation for Data Protection under the Act. In August, 2005, the Expert Committee submitted its report which was based upon the interactive sessions with various interest groups, deliberations of the Inter Ministerial Group comprising representatives of Ministries/Departments concerned with the subject matter, presentation made by NASSCOM and feedback on the publication of the report on the DIT website.

8. Now, the Government was left with two approaches i.e. either to enact new and exclusive legislations or to amend the existing legislations to encompass the new crimes and to enact specific legislations to address the issues if amendments to the existent laws do not suffice. As the second approach required minimum effort, the Government preferred it by creating a few more provisions in the Information Technology Act, 2000 and some supplementary provisions by making amendments in other Acts such as the Indian Penal Code and the Code of Criminal Procedures, 1973.

9. Thus, the Information Technology (Amendment) Bill, 2006 was introduced in Parliament on 15.12.2006 and referred to this Committee for detailed examination and report. In the process, the Committee received several write

ups from and heard the views/suggestions of numerous individuals, experts, associations, industry representatives, Central Bureau of Investigation (CBI), Ministry of Law and Justice (Legislative Department) and the Department of Information Technology. After considering and paying due attention to such views/suggestions and clarifications, the Committee have attempted in this Report to suggest and recommend certain measures to be taken by the Government for making the law more effective and comprehensive.

I. Self Enabling and People Friendly Laws

10. Upon receipt of several suggestions from various quarters that the Information Technology Act should be self enabling instead of leaving several provisions to be taken care of by the Indian Penal Code (IPC), Criminal Penal Code (Cr. P.C.) etc. as computers did not exist when these laws were formulated, the Committee desired to hear the views of the Department of Information Technology. In reply, it was stated that at the time of the drafting of the principal Act in 1998, the experts were of the opinion that Acts like IPC, Cr. PC, were primary and basic Acts which were very appropriately worded and had passed the test of time. It was further stated that several other legislations framed over the last fifty years used to refer to these basic Acts. Moreover, the law enforcement agencies and the courts very well understood these Acts and the issues involved therein.

11. The Committee, during the evidence, asked whether it would not be very cumbersome to refer to a number of provisions contained in other Acts when a cyber crime was committed. In response, the Secretary, DIT stated:-

> "In terms of definition, they are too closely linked. Say, if you talk of impersonation, in our Act, we have to follow a similar set of provisions, a similar set of definitions which are used in IPC."

12. The Committee, then queried about the provisions contained in the Bill to make the law people friendly in view of the major trend the world over to have such comprehensive laws which would easily be understood by the common man and having least dependence on other laws. In reply, it was stated that the necessity of the people friendly law was the main guiding principle before the Department in suggesting appropriate provisions in the Information Technology (Amendment) Bill, 2006.

13. It was further stated that in order to make the law more people friendly, the punishments had been rationalized in some of the offences. Such rationalization would help in the growth of the IT Industry and check undue harassment of the ignorant citizens, not aware of the nuances of cyber laws.

14. On the issue of bringing a self enabling and people friendly law instead of referring to the provisions contained in the other laws, the Ministry of Law of Justice (Legislative Department) were of the opinion that the legislative practice to criminalise certain acts or omissions as an offence under the Indian Penal Code and in the Information Technology Act, 2000 seemed to be working well and the same should continue.

II. Cyber Crime and Cyber Terrorism

15. During the course of the examination of the Bill the Committee were informed by some legal experts/industry representatives that the proposed amendments did not put much focus on cyber crimes including cyber terrorism and their coverage was not at all commensurate with the requirement. Citing some example they stated that although morphing was taking place across the country, yet there was not a single direct provision under the proposed amendments to make morphing a penal offence punishable with imprisonment and fine. Similarly, there was no specific provision to make cyber terrorism a punishable crime.

16. In the above context, the Committee desired to know from the Department that whether it was not necessary for India, as a sovereign nation, to enact a specific law making morphing, cyber terrorism and other similar cyber crime penal offences punishable with the highest fine and imprisonment. In reply, the Department stated that a provision to make cyber terrorism a punishable crime with highest fine and imprisonment similar to the lines of Section 121 and Section 120 B of IPC might be considered, as the punishment with imprisonment of either description for a term which might extend to 10 years is the highest imprisonment terms given for any offence under the IT Act. It was also stated that morphing would get covered in sub-clause (1) of Sections 43 and 66.

17. In evidence the Committee asked whether 'cyber terrorism' has been defined anywhere in the IT Act, 2000 or in the proposed amendments. The representative of the Department replied in the negative.

III. Jurisdiction of the Law

18. In the context of the reported cyber offences committed outside the country, the Committee attempted to look into the jurisdiction and applicability of the IT Act, 2000. Section 1(2) of the Information Technology Act says "It shall extend to the whole of India and save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person". Similarly, Section 75 provides as under:-

> Act to apply for offence or contravention committed outside India-
> (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
> (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

19. In the above context, while taking evidence of a legal expert in cyber crimes, the Committee desired to know the effectiveness of enforcing the above provision to the cyber crimes perpetrated abroad. In reply the expert stated:-

> ".....Section 75 brings some sanity to that approach by saying it will only apply so long as it impacts a computer, a computer system or a computer network that is physically located in India. So, as a sovereign nation, there is nothing stopping India to enact a law making the cyber terrorism as a specific offence punishable with the highest imprisonment."

20. Asked to state specifically how could the Indian State enforce its will within the domain of another sovereign nation, the witness replied that it was a practical problem. The Committee, then, asked whether there was any practicable way out to deal with this tricky situation. In reply, the witness stated that the USA was effectively assuming jurisdiction over computers located

outside its domain on the ground that the activity of those computers impacted the computers physically located in the USA. The witness further stated that another option could be that India should join some of the global treaties like Convention on Cyber Crime or Group 7. He added:-

> "In the internet space there is one specific agency which is known as International Corporation for Assigned Names and Numbers. In short, it is known as ICANN. It is a global body that manages internet. However, it has steered clear of any controversy of even contributing towards cyber crime regulation. It does have a Committee known as the Government Advisory Committee of which India is already a Member."

21. He summed up by stating that as ICANN/Government Advisory Committee was dealing only with the policy issues concerning internet and had not gone to the direction of regulating cyber crime *per se*, the practical problem of ensuring the physical presence of the alleged perpetrators of cyber crime from abroad still persisted.

22. In the above context, a representative of the Central Bureau of Investigation (CBI) while deposing before the Committee stated that apart from specific provisions in the Information Technology Act, there was a basic law and Sections 3 and 4 of the Indian Penal Code could take care of this eventuality.

23. Asked to state categorically the means by which the jurisdiction of Indian laws could extend beyond its boundaries, the witness stated:-

> ".....jurisdiction is not an issue because even without specific provisions in this statute, Sections 3 and 4 (of IPC), if interpreted properly, have enough scope and cover wide area.....Now the question is that if a New Zealander sitting in New Zealand commits an offence under this law which impacts India, perhaps on this point, I would say it is a bit tricky and we will have to understand frankly."

24. The Committee desired to know whether it would be appropriate for India to have an extradition treaty especially in respect of cyber crime or should there be a special International Convention on cyber crime to make it obligatory on the part of the signatories to extend mutual cooperation. In response, another representative of CBI submitted that it was high time that India considered becoming signatory to such an International Treaty/Convention, otherwise, it would be extremely difficult to book the perpetrator of cyber crime sitting abroad.

25. The Ministry of Law and Justice (Legislative Department) on the issue of dealing with the cyber crimes perpetrated abroad but impacting India, stated that Sub-Clause (a) of Clause 49 of the Information Technology (Amendment) Bill, 2006 sought to insert sub-section (3) in Section 4 of the Indian Penal Code so as to extend the jurisdiction of the IPC to any person in any place without and beyond India committing offence by targeting a computer resource located in India. Further, the main thrust of Section 75 of the Information Technology Act and the proposed sub-section (3) of Section 4 of IPC was to criminalize those acts of persons which might have an impact on any person and property situated in India.

26. Not convinced, the Committee asked whether the physical presence of the alleged accused in a criminal prosecution was not necessary. In reply the Legislative Department submitted that in a criminal prosecution, the physical presence of the alleged accused was necessary and the same might be ensured through international cooperation and bilateral extradition treaties.

27. The Committee, then, decided to hear the views of the Department of Information Technology on this perplexing issue. The Department, in reply, stated that all the countries world over had expanded the jurisdiction of their cyber laws to offences or contraventions committed on their systems in the country from outside the country. Following such a practice, India had also provided Section 75 in the Information Technology Act for offences or contraventions committed on systems in India from outside the country. It was also stated that the Governments all over the world had also taken recourse to enter into treaties to bring to book the cyber criminal outside the territorial jurisdiction of their country. India, on its part, had also made efforts to enter bilateral agreements with foreign countries to deal with the cyber crimes committed on Indian systems from foreign lands. Cyber crime treaties were stated to be covered under the Mutual Legal Assistance Treaties (MLATs). India is also a member of Cyber Crime Technology Information Network System (CTINS) a Japanese Government initiative for mutual exchange of information regarding cyber crimes among the member countries which is, of course, advisory in nature.

28. Asked to specify whether it would be prudent for India to become a signatory to any unilateral International Treaty or Convention on Cyber Crime to effectively implement the law, it was replied that international cooperation in the form of mutual legal assistance would require an international agreement or other similar arrangements such as reciprocal legislation. It was further stated that such provisions, whether multilateral or bilateral, would oblige authorities of the contracting party to respond to the request for mutual legal assistance in the agreed case. It would, therefore, be necessary for India also to become a signatory to any international treaty or an international convention on Cyber Crime on the mutually acceptable terms.

29. In response to a specific query with regard to the number of countries with whom India had already entered into Mutual Legal Assistance Treaties (MLATs), it was replied that with seventeen countries India had already entered into such treaties, with five countries treaties had already been signed but the same had yet to come into force and with four countries treaties had already been finalised/initiated but the same were awaiting signature.

30. The Committee asked how action could be taken against the alleged perpetrator of cyber crime taking shelter in those countries with which India did not have any extradition treaty. In reply, the Secretary, DIT during evidence submitted:-

> "There are provisions in the general laws. I assume we cannot go beyond those general laws.....whatever is to be done in the light of cyber crime, it must be done within the framework of what is being done for a general law and outside law."

IV. Substitution of 'digital signature' by 'electronic signature' (Clause 2)

31. Clause 2 of the Information Technology (Amendment) Bill, 2006 says "In the Information Technology Act, 2000 (hereinafter in this Part referred to as the principal Act), for the words "digital signature" occurring in the Chapter, section, subsection and Clause referred to in the Table below, the words "electronic signature" shall be substituted.

TABLE

S. No.	Chapter/section/sub-section/Clause
1.	Clause (*d*), (*g*), (*h*) and (*zg*) of section 2;
2.	Section 5 and its marginal heading;
3.	Marginal heading of section 6;
4.	Clauses (*a*), (*b*), (*c*) and (*e*) of section 10 and its marginal heading;
5.	Heading of Chapter V;
6.	Clauses (*f*) and (*g*) of section 18;
7.	Sub-section (*2*) of section 19;
8.	Sub-sections (*1*) and (*2*) of section 21 and its marginal heading;
9.	Sub-section (*3*) of section 25;
10.	Clause (*c*) of section 30;
11.	Clauses (*a*) and (*d*) of sub-section (*1*) and sub-section(*2*) of section 34;
12.	Heading of Chapter VII;
13.	Section 35 and its marginal heading;
14.	Section 64;
15.	Section 71;
16.	Sub-section (*1*) of section 73 and its marginal heading;
17.	Section 74; and
18.	Clauses (*d*), (n) and (*o*) of sub-section (*2*) of Section 87.

32. In the above context, the Committee received views from some experts/associations that while the law talked about 'electronic signature' in a couple of sections, in reality it was still continuing on 'digital signature'. They opined that mere replacement of the term 'digital signature' by the words 'electronic signature', as proposed in the Bill would not be enough and it had to be followed in spirit also.

33. One of the experts while tendering evidence before the Committee submitted:-

> "..... while the law has made it technologically very sound by providing for electronic signatures, there is a slight disconnect..... what I am trying to say is that while we are talking of big generic electronic signature which includes digital signature and lot of other things, the law effectively continues to be law of digital signatures.. Either we can use a language or we can suggest to the Government for illustration, the digital signature regime is detailed."

34. Asked to state categorically how electronic signature could be followed in letter and spirit, the witness replied that biometrics needed to be an integral part of it.

35. On the issue of 'electronic signature' the Ministry of Law and Justice (Legislative Department) have stated that Information Technology Act, 2000 defines 'electronic signatures' to mean authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature. The Information Technology Act, 2000 confers power on the Controller to supervise the activities of the certifying authorities. Statutory provision obliging certifying officers to follow certain procedure has also been made in section 30 of the Act. The Information Technology Act, 2000 and the Information Technology (Amendment) Bill, 2006 put emphasis on reliable electronic signatures and enable the Central Government to take necessary steps keeping in view the needs of emerging technologies.

36. Taking cognizance of such views/suggestions the Committee desired to be apprised of the views of the Department of Information Technology for enforcing 'electronic signature' in letter and spirit. In reply, it was stated that the United Nations had passed a resolution in the year 2001 recommending that all States should give favourable consideration to the Model Law on 'Electronic Signatures' when enacting or revising there laws in view of the need for uniformity of the law applicable to alternatives to paper based methods of communication and storage of information.

37. The Department further stated that 'digital signature', as a matter of fact, has been one of the types of 'electronic signature' and based on the technologies available. 'digital signature' has been found to be one of the most reliable methods for security, integrity and authentication of electronic records. However, since the technology is an ever-evolving process, there could be such technologies which could be used as a reliable method for the electronic records. Moreover, as it is difficult to amend the Act very frequently, and hence for future technologies, a provision has been made for incorporating those technologies for 'electronic signatures' under the proposed Second Schedule of the Bill.

38. The Committee asked about the mechanism put in place to guard against forgery of digital signatures. The representative of the Department of Information Technology submitted in evidence:-

> ".....there are two parts as far as the digital signature is concerned ..... One is the user experience and the other is, what is

actually happening at the back. These are two different parts, both of which have been touched upon..... In Karnataka for example, the entire land records have been digitalized. They are now securely stored; there is no difficulty in verifying whether a particular record has been signed by that particular Revenue Official. They have the tracking, they use biometric.....they are well Protected by all these methodologies and there is no difficulty..... But when we talk about translating that into a piece of paper and getting a printout and then try to adopt the same value to the printed paper, then there are issues."

39. Asked to specify the mechanism developed to check tampering or fraud of digital signature the representative of DIT replied:-

"Sir, in the digital records, which are stored, there is a mechanism to audit it, which shows every change that has been made; who has changed it; on what date it has been changed."

V. Auditing of electronic Records

40. Some of the industry representatives suggested to the Committee that there should be an auditing of all the electronic records in order to have legal sanctity as well as to check frauds that are constantly occurring in corporate India. The representatives further stated that it would also help in bringing far more clarity to the entire regime of proof of electronic records.

41. In the above context, when the Committee desired to hear the views of the Department of Information Technology, it was replied that the suggestions made by the industry representatives seemed to be appropriate. It was further stated that the Comptroller and Auditor General of India had already started conducting Information Systems Audit of Government Organisations, Departments, PSUs, Autonomous Bodies and Authorities for evalution of acquisition and installation of the computer and computer systems, systems effectiveness, security, economy, efficiency and data integrity and compliance of system related activities with applicable laws, regulations and guidelines.

42. Asked to indicate the global practice relating to the auditing of the electronic records, the Department replied that it would have been better if the concerned industry representatives provided more details regarding the global practices and standards in this regard as there would be a need to setup process, practice and standards in line with those prevailing in international arena for undertaking such audits.

43. One of the representatives of the industry while tendering evidence before the Committee stated in this regard that globally auditing of electronics records was being done. He also stated that there were two independent streams of auditing, one relating to the information systems and the other to information security.

VI. Definition and Role of Intermediary & Liability of Network Service Providers

(Clauses 4 & 38)

44. Section 2 (w) of the principal Act defines "intermediary", with respect to any particular message as any person who on behalf of another person receives, stores or transmits that message or provide any service with respect to that message.

45. Clause 4. sub-Clause (F) of the Bill proposes to amend the above definition of 'intermediary' as follows:-

"(w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes, but does not include body corporate referred to in section 43 A.

46. Further, Clause 38 of the Bill intends to substitute chapter XII of the principal Act whereby the intermediaries will not be made liable in certain cases. The said Clause reads as follows:-

"For Chapter XII of the principal Act, the following Chapters shall be substituted, namely:-

CHAPTER XII

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

(1) Notwithstanding anything contained in any other law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary

shall not be liable for any third party information, data, or communication link made available by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not—

(i) initiate the transaction,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission.

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

(4) Intermediary shall observe such other guidelines as the Central government may prescribe in this behalf.

Explanation.-For this purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary."

*****	*****	*****	*****
*****	*****	*****	*****
*****	*****	*****	*****

47. In the above contexts, some of the experts/industry representatives were of the view that the definition of 'intermediary' was not clear which was bound to create a problem of interpretation as to who would be an intermediary. So much so that under the existing definition, even an employer would become an intermediary.

48. One of the experts/industry representatives who tendered evidence before the Committee stated:-

> "Currently the network service providers are made liable for all third party content or data. In the proposed one, they are not being made liable at all except when it is proved that they conspired or abetted. How does the Government expect a normal citizen to prove conspiracy or abetment by network service provider?"

49. The Committee desired to hear the comments of the Department of Information Technology on the above issue of properly defining the terms 'intermediary' and its role. In reply, it was stated that Section 79 of the principal Act had been revised in line with those provided for similar provisions in the European Act. Sub-section 4 of Section 79 of the Act has empowered the Central Government to provide guidelines which may be observed by the intermediary. These guidelines would vary from time to time keeping in view the new services, technologies and circumstances. Accordingly, guidelines were stated to be proposed for prescription through the rule making powers.

50. Not convinced, the Committee asked during evidence what actually constituted the 'intermediary'. In reply, a representative of the Department of IT stated that any service provider was an intermediary. In that case, the Committee asked the rationale for intermediaries/service, providers being not made liable in certain cases. In reply, the representative of DIT stated:-

> ".....any of the service provider may not be knowing exactly what their subscribers are doing. For what they are not knowing, they should not be penalised. This is the provision being followed worldwide."

51. Asked to elaborate, the witness stated that the intermediaries or service providers did not have anything to do with what was passing or returned through their network. But if they selected or changed or modified any content, then they would not be covered under the instant Clause.

52. The Committee then desired to know the mechanism evolved to establish conspiracy or abetment on the part of the intermediaries/service providers. In reply, it was stated that the proposed Section 79 did not absolve the network service providers from civil liabilities. It was also stated that the exemption of intermediaries from liability had been clearly defined in the proposed sub-sections 2&3 of Section 79. Further, sub-section 4 empowered the Government to prescribe guidelines which were to be observed by the intermediaries.

53. The Committee asked whether the possibility of suing or getting information from the service provider would cease to exist in the eventuality of proposed Section 79 being put in place. In reply, it was stated that any consumer could sue the network service providers for civil liabilities.

54. During evidence, the Committee asked whether it would not be extremely difficult to establish conspiracy or abetment in order to sue the intermediaries/service providers. In reply, the representative stated:-

> "It becomes very difficult. Sir, you are right."

55. The Committee then queried whether it would not be prudent to cast some minimum obligation/responsibility upon the intermediaries/service providers when their platform was being abused for transmission of obscene and objectionable contents. In reply, a representative of, DIT stated:-

> "Unfortunately, at the discussion that we were having on the IT Act, the general consensus was that the intermediary should not be put under such an obligation. That is why, we have incorporated it. Now that we have your views, I think we will really look at it."

56. When the Committee desired to have the views of the Legislative Department as to whether they were satisfied with the term 'intermediary' and its role as defined in the Bill, they just defined the term as spelt out in the Bill and stated that there were many aspects of intermediaries which would result in criminal liability and Civil liability and the Information Technology (Amendment) Bill, 2006 provided for adequate safeguards in this regard.

57. The Central Bureau of Investigation (CBI) on the above issue stated that the Bill sought to remove the 'due diligence' Clause for claiming immunity by the intermediaries. Elaborating the ramifications, they stated that in the real world some liabilities existed on the owner of a premise for prevention of certain types of criminal offences including sale of contraband goods. Absence of any such obligation would, therefore, place the intermediaries such as online auction sites/market places in a privileged position and disturb the equilibrium with their counter part real life entities. Also, quite often the damages caused to the victims through reckless activities in the cyber world used to be immense and irreparable. The CBI, therefore, suggested that the intermediaries should be divided into two classes i.e. online Market Places/Auction sites, and the rest. Entities in the former class of intermediaries should not be given immunity

unless they proved due diligence which might be exercised by them through technical scrutiny of traffic data through filters for removing hate content, obscene material, sale of contraband goods, etc..

58. Asked to comment on the rationale behind removing the words 'due diligence' and the above views/suggestions of the CBI, the Department of Information Technology stated that the words 'due diligence' were provided in section 79 of the IT Act as it was felt that it had been adequately and properly defined by the Supreme Court of India. However, while suggesting amendments to the IT Act, it was felt that the provisions under Section 79 pertaining to exemption from liability of network service provider should be explicitly defined. Further, the sub-section 4 of Section 79 has empowered the Central Government to provide certain guidelines which would be observed by the network service providers. The words 'due diligence' could be covered under those guidelines.

Obligations on body corporates

59. As regards casting obligation of paying damages through compensation only on 'body corporates', it was clarified by the Department that this issue was extensively debated by the Expert Committee according to whom it was a well thought idea to restrict the Section to the body corporates alone. The Department further stated that once the system was put in place, it might be considered to extend the Section to the individuals and persons.

60. A representative of the Department of Information Technology supplemented in evidence:-

> ".....But basically we are really to satisfy the customers who are doing outsourcing or asking call centres to be operated and they should be given protection. This would help business in general. Most of such businesses or almost all the business is done only by body corporate. To that extent, provision which is being made will be adequate."

61. Asked to state, whether the industry representatives were consulted while fixing obligations on the body corporate, a representative of the Department stated in evidence that NASSCOM and other industry people were consulted on the issue.

VII. Contraventions of serious nature
(Clause – 19)

62. Section 43 of the IT Act, 2000 reads as under:-

"Penalty for damage to computer, computer system, etc.- if any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network-

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

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

(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such 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 authorized to access any computer, computer system or computer network by any means;

(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

63. Clause 19 of the IT (Amendment) Bill, 2006 proposes to amend section 43 of the principal Act. The Clause reads as follows:-

"In section 43 of the principal Act, -

(a) in the marginal heading, for the word "Penalty", the word "Compensation" shall be substituted;

(b) after Clause (h), the following Clause shall be inserted, namely:-

"(*i*) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means,".

64. In the above context, the Central Bureau of Investigation (CBI) opined that contraventions enumerated in Clauses (c) to (i) have been serious in nature. They, therefore, suggested that while contraventions enumerated in Clauses (a) & (b) of Section 43 might remain as proposed, the contraventions enumerated in Clauses (c) to (i) may be made punishable with imprisonment for 3 years and fine.

65. The Committee sought the views of the Department of Information Technology in this regard. In reply, it was stated that the contraventions listed in (c) of Section 43 were of civil nature where damages were payable by way of compensation to a maximum extent of rupees one crore. The contraventions have also been made criminal offences in Section 66 of the Bill with imprisonment and fine.

VIII. Compensation for failure to protect data (Clause 20)

66. Clause 20 of the Bill proposes to insert a new Section 43 A regarding compensation for failure to protect data. The Clause reads:-

"After Section 43 of the principal Act, the following section shall be inserted, namely:-

'43 A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful

gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Explanation.-For the purposes of this section,-

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultations with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.'

67. In the above context, the Committee received a number of suggestions from individuals experts/industry representatives. The main suggestions were as follows:-

i) It should be clarified what would constitute 'wrongful loss' or 'wrongful gain' in all instances;

ii) It should be extended to any situation when the body corporate fails to maintain the reasonable security practices and procedure;

iii) The obligation to pay damages by way of compensation should also extend to any person operating the information alongwith the body corporate owning or controlling personal information;

iv) Some mechanism should be put in place by the means of which the affected individual is informed about the breach and other details;

v) An empowering provision should be made in this Section to authorize appropriate Self Regulatory Organisations (SROs) to evolve proper

approaches in order to foster a healthy information security culture through education backed by demonstrative enforcement.

(i) Wrongful loss or wrongful gain

68. In response to the above, the Department of Information Technology stated that the words 'wrongful loss' or 'wrongful gain' have been provided in tune with the Indian Penal Code (IPC). These terms have been well defined under Section 23 of the Indian Penal Code. The Department also stated that Section '2' of the principal Act had provided for definition of 'information', 'data' and 'computer' which would be valid both for online and offline activities.

(ii) Quantum of damage through compensation

69. Taking cognizance of the amount of fine not exceeding Rs. 5 crore, as prescribed in the proposed Section 43 A, on body corporates being negligent in implementing and maintaining reasonable security practices and procedures, the Committee desired to be apprised of the rationale for fixing the damages by way of compensation at Rs. 5 crore. In reply, a representative of the Department submitted in evidence:-

> ".....a person who has committed a contravention, is liable to pay compensation to a victim to the maximum of Rs. one crore in the existing Section 43 of the Act. Now through Section 43 A, it is proposed to make the body corporate who acquires the data or possess the data or process the data also liable, in case there is any data theft. He needs to implement the best security practices to protect the data from leakage. In case of any contravention, the body corporate will have to pay rupees five crore."

70. Appreciating the enhancement of damages from the originally prescribed rupees one crore, the Committee specifically desired to know how the figure of rupees five crore was arrived at especially in view of, say, at least a thousand crore rupees flourishing IT industry. The representative replied:-

> "Sir, in fact, the figure of about Rs. 25 crore was suggested initially. Then, I think, the industry said 'now we should keep it low'. Then Rs. 5 crore was kept there. This is the factual position."

71. Expressing their concern, the Committee asked whether there could be a concept of 'cap' on damages prescribed under the law. The representative of the Department replied that no capping on damages was intended. Rather a

provision was being made that over and above the amount of Rs. 5 crore, the Court could grant additional compensation to the victim.

72. Asked to indicate the mechanism evolved for imposition of the damage of rupees five crore, the representative of the Department replied that first the victim would go to the Adjudicator, then to the Cyber Tribunal and if still dissatisfied he could go to the High Court and Supreme Court.

73. The Committee asked whether the entire process was not very cumbersome. A representative of, DIT replied:-

> "Sir, about implications under the Act, the Tribunal and the Adjudicator can award at best Rs. 5 crore."

74. He further submitted:-

> "We shall immediately look into the views of the Members on the enhancement and we will get back after consulting the industry."

75. In this context, the Committee desired to have the views of the industry about the basis in which they recommended to reduce the fine to Rs. 5 crore from the original proposal of Rs. 25 crore. In reply, one of the industry representatives submitted in evidence:-

> ".....In not a single case in the last several years even one rupee damage by way of compensation has been awarded in India. That really erodes the confidence of the community and corporate India on this so-called effective remedy of providing damages by way of compensation."

76. In a subsequent evidence, another industry representatives supplemented:-

> ".....the best deterrent is certainty of punishment and not necessarily the extent which may be somewhat open ended.....with the little experience that we have seen if you have very severe punishment, then in cases where the evidence is not completely full proof, where it is somewhat circumstantial, the court takes a view, quite rightly, of giving the benefit of doubt to the defendant."

77. They summed up by stating that Rs. 5 crore as prescribed under the law seemed to be a sufficient deterrence.

78. Asked to indicate similar penalty provision that were being followed in advanced countries, one of the industry representatives submitted:-

> "Sir, we have not greatly studied this point, but the contracts that are entered into impose high penalty for any breach. They are all

subject to the jurisdiction of the Courts in other countries. So, other countries have a history of awarding damages which our Courts do not do. Considering that, it is a reasonable amount. But we are not really experts in it."

(iii) Stolen Data- prosecution of recipient.

79. A number of suggestions were received from various quarters that a suitable provision should be incorporated in the Act to prosecute the recipient of stolen data.

80. In the above context, when the Committee desired to have the views of the Department of Information Technology, it was replied that an appropriate provision in this regard might be considered for incorporation in the Act.

81. The Legislative Department, when asked to furnish their comments, stated that the provision for this purpose could be considered favourably as there was no specific provision in the IT Act which prescribed prosecution of persons receiving the stolen data.

(iv) Data Protection and Retention

82. Several suggestions were received from various industry representatives that the proposed amendments have completely been silent on data protection. The industry's contention was that as there was no adequate provision of data protection in India as compared to the level of such protection available in Europe, the law here was turning out to be a stronger anti-outsourcing legislation.

83. The representatives further submitted in evidence that the enabling data protection provision should include 'sensitive personal data' as defined by the European Union. Asked to distinguish between 'personal data' and 'sensitive personal data', an industry representative stated that essentially it was derived from the European Union Data protection directive which distinguished between 'personal data' and 'sensitive personal data'. While 'personal data' has been defined in a much more generic manner, 'sensitive personal data' has been exhaustively defined as 'personal data consisting of information as to the racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of the trade union, his

physical or mental health or condition, his sexual life, the commission or alleged commission by him or any offence and proceeding for any offence committed or alleged to have been committed by him, the disposal of such proceedings for the sentence of any court in such proceedings.'

84. The industry representative summed up:-

> "So, the point we are trying to make here is essentially that when we are talking about sensitive personal data here and in the future should we come up with the data protection legislation, then there would be no inconsistency between what is brought about there and what is brought about here."

85. Some other experts/associations who deposed before the Committee were of the opinion that 'privacy' as a concept, had not been defined under the explanation or the definitional Clause or under the proposed Section 72 in the manner expected. Asked to elaborate, one such representative submitted during evidence that 'privacy' in today's context needed to be classified into two kinds i.e. 'personal privacy' and 'data privacy'.

86. On the issue of data protection, when the Committee desired to have the views of the Legislative Department, they stated that in the context of the protection of intellectual property rights, there is no provision in the present Bill to protect the data. Copyrights and Patents traditionally conferred property rights in "expression" and "invention" respectively. Ideas and facts remained in public domain for all to draw on and to innovate a new one. Data protection legislation confer database rights over facts, business method and software patents. The competing challenges are the property protection on data exclusivity and demand for more areas in public domain so that creativity may grow. These are hard policy options and legislative Department leaves it to the administrative Ministry to take decision in the matter.

87. As regards data retention, the Legislative Department stated that data retention was as important as data protection. Therefore, it was highly desirable that the protected data should be retained for a specified period. The retention of accurately recorded and retrievable research data was of utmost importance for the progress of scientific integrity. The investigator must have clearly defined responsibility for recording, retaining, and storing research data. The data retention was essential for following reasons:-

(a) In the interests of national security;

(b) For the purpose of preventing or detecting crime or of preventing disorder;

(c) In the interests of the economic well-being of India;

(d) In the interests of public safety;

(e) For the purpose of protecting pubic health;

(f) For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

88. The Legislative Department further stated that the Information Technology Act, 2000 has only one section relating to retention of electronic records i.e. Section 7 which provides that where any law provides that document, record or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information is retained in the electronic form. the term 'information' is defined in the Act to include data, text, images, sound, voice, codes, computer programme, software and data bases or micro film or computer generated micro fiche.

89. The Legislative Department concluded by stating that thus this Section did not specify the period for which the data was to be retained but provided that if any other Act provided for data retention for a specific period then if the data was retained in electronic form that requirement shall be deemed to have been satisfied.

90. The Department of Information Technology agreed that it would be appropriate to provide for an enabling data protection and retention legislation. They also agreed to the proposal that 'personal privacy' or 'individual identity privacy' should find a place alongwith 'data privacy'.

IX. Amendment of Section 61 (Powers to Civil Courts) (Clause 29)

91. Section 61 of the principal Act says "No Court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."

92. Clause 29 of the Bill proposes to amend the above Section by saying "Provided that the Court may exercise jurisdiction in any cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter."

93. In the above context, the industry representatives submitted to the Committee that the circumstances under which the Civil Court's role would come into play should be clarified. They further suggested that it should also be clarified whether the Civil court could restrict the jurisdiction of the tribunal in the present case.

94. Asked to comment upon the above suggestions of the industry representatives, the Department of Information Technology submitted that it would be appropriate to suggest that the Adjudicating Officer would transfer the cases, where the damages claimed have been more than Rs. 5 crore, to an appropriate Court.

X. Quantum of Punishment [(Clauses 31, 36, 37, 49 (e), 49 (h) and 51 (a)]

95. Clause 31 of the Bill proposes to amend sections 66, 67 & 67 A whereby the quantum of punishment for cyber crimes would be reduced to two years and thereby be made non-cognisable.

96. Similarly, Clause 36 of the Bill proposes to insert a new Section 72 A where offences would be made non-cognisable. Clause 37 intends to substitute Section 77 & 78 of the principal Act by new Sections 77, 77 (A), 77 (B) and 78.

As per the proposed Section 77 (A), offences created under Sections 66, 66 A, 72 and 72 A would be made complaint offences.

97. *Vide* Clause 49 (e) of the Bill, Section 417 A is proposed to be incorporated in the IPC to criminalize cheating by using the electronic signatures and password etc. However, this offence has been made non-cognisable.

98. Likewise, *vide* Clause 49 (h) of the Bill, Section 502 A of the principal Act is proposed to be incorporated in the IPC to criminalize invasion of privacy by imaging and transmission of private parts of someone. This offence has also been made non-cognisable.

99. Moreover, Clause 51 (a) of the Bill proposes to add a new Section 98 D in Cr.P.C. vide which no court shall take cognizance of an offence punishable under Sections 417 A, 419 A and 502 of IPC except on complaint of the aggrieved. However, offences under 417 A and 502 are proposed to be made non-cognisable.

100. The Central Bureau of Investigation (CBI) while commenting upon the aforesaid provisions suggested that offences under all the above Sections should be made cognizable. Some industry representatives were also of the same view.

101. Taking into consideration the above suggestions, the Committee desired to know from the Department of Information Technology the rationale for reducing the quantum of punishment under various Sections, as enumerated above. In reply, it was stated that to provide clarity in interpretation of the offences and damages, the provisions of Section 66 have been expanded keeping the existing provision pertaining to hacking. The contraventions in Section 43 have been mapped as offences in Section 66. Attempts have been made to rationalize the punishments in line with the Penal Code.

102. It was further stated that the growth and progress of the IT industry has been because the Government has played only a supportive role, and has consciously kept out of regulating the industry. Similarly, the growth of the Internet and its utility has been because it has been a completely uncontrolled medium. Moreover, the Government is trying to enhance usage of PCs and the Internet, is launching a massive e-Governance programme, and is working towards bridging the digital divide. Except a handful of users, the majority may

be abysmally ignorant of the nuances of cyber laws. While penal provisions are necessary to prevent flagrant abuse of the system, care has to be taken that such provisions do not give occasion for harassment of legitimate users and the common man. Such an approach would only scare users, thereby defeating the efforts of the Government to proliferate e-Governance and increase use of Information Technology for better productivity. The Government might well lose the tremendous advantage that they now enjoy in this field. Punishments have been rationlised keeping these factors and the established norms of Indian legal system in mind. It was felt that there should be a need to create a balance between the Indian Penal code and IT Act, 2000.

103. The Department summed up by stating that attempts have been made to rationalize the punishment of offences. The punishment of three years in general as provided in the IT Act was made cognisable and bailable. The whole idea of rationalizing the punishment was that the person should be able to get a bail.

104. In evidence, raising the same issue the Committee asked about the immediate provocation on the part of the Government to reconsider its own earlier proposal of keeping the term of imprisonment at three years. A representative of the Department submitted that the issue was that people were not getting bails in the court of law.

105. Expressing their surprise the Committee asked whether the Department was trying to be criminal friendly and desired to know whether a provision could be incorporated whereby imprisonment of three years could be made bailable in case of first offence and non-bailable in subsequent offences. The representative of DIT replied.

> "We tried the Law Ministry. In the Circular, Schedule II of the Cr. PC, they say it is not amendable. That is why the whole issue came up there".

106. When the Ministry of Law & Justice (Legislative Department) were asked to give their opinion on the above issue, it was stated that the penalty provisions as proposed under various Clauses seemed to be adequate.

XI. (i) Definition of terms 'dishonestly' and 'fraudulently' (Clause 31)

107. Clause 31 of the Bill proposes to amend Section 66 of the principal Act by saying "If any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable....." The said Clause explains that the words 'dishonestly' and 'fraudulently' shall have the meaning assigned to them in Sections 24 and 25 respectively of the Indian Penal Code.

108. In the above context, the Committee received suggestions to the effect that merely going by the definition of the terms 'dishonestly' and 'fraudulently' as in the IPC might not be an appropriate way to deal in the new law.

109. Asked to comment, the Department of Information Technology stated that both the terms 'dishonestly' and 'fraudulently' were being used in reference of the crime. The existing definitions for these two terms in IPC have been proposed to be used in the Information Technology Act. Law Ministry has suggested that the definition for terms like 'fraudulently' 'dishonesty' as appear in IPC should be incorporated in the Information Technology Act so that any confusion, as well different interpretation of these two terms w.r.t. crime at any point of time could be avoided by different courts in the country.

110. The Department further stated:-

> "We would like to retain the definition of terms like 'fraudulently' and 'dishonesty' in line with IPC as the courts very well understand interpretation of these definitions in reference of crimes and offences"

111. In evidence, the Committee asked whether some terms like 'dishonestly', fraudulently', impersonation', while dealing in the cyber process were not different from what was ordinarily understood in the general penal law of the land. The Committee further desired to know whether it would not be appropriate to define the above terms in the IT Act itself. The Secretary, DIT replied:-

> "Then the pronouncement of the courts would have to apply slightly differently to the IT Act and slightly differently to the IPC."

(ii) **Omission of the word 'hacking'**

112. Clause 31, while intending to amend Section 66 has proposed to delete the word 'hacking'. In this regard, the Committee received a number of representations that there has been no rationale in deleting the offence of hacking under Section 66 of the existing law as the current provisions of that Section of the principal Act have been very wide to fight newly emerging kinds of cyber crimes.

113. A representative of the industry while deposing before the Committee stated in evidence:-

> ".....If it is deleted or made extremely narrow by the proposed Section 66(1) which is talking about dishonestly or fraudulently doing the act, then the interest of corporate India may not be appropriately met....."

114. A retired Secretary, R&AW was also of the same view and stated in evidence that the proposed amendment to delete 'hacking' would seriously affect the capability of the law enforcing agencies/officers to bring to book the offenders violating the IT Act. He was, therefore, of the view that 'hacking' should remain in its present form.

115. The Committee desired to hear the comments of the Department of Information Technology on the above suggestions. In reply, it was stated that the word 'hacking' was more a colloquial word and would change over a period of time. It was further stated that all features of 'hacking' have been adequately covered in Clauses 19 (Section 43) and 31 (Section 66).

116. In evidence, a representative of the Department of Information Technology stated that all the features of hacking were there and only the word 'hacking' was removed.

117. The Committee asked the need for removing the word 'hacking' which was already there in the Act. The representative of the Department replied:-

> "Sir, the reason is this. Earlier, the word 'hacking' appeared in Section 66 as a criminal offence. Hacking is normally taken to be a criminal offence. Now, since Section 43 A is more a civil kind of thing there, we are mapping one-to-one Sections 43 and 66 together and so we removed the word 'hacking' so that there is no seamless mapping in both the Sections. Otherwise there is no reason."

(iii) **Child Pornography**

118. Clause 31 proposes to insert Section 67 A whereby punishment has been provided for publishing or transmitting of material containing sexually explicit act in electronic form.

119. In the above context, a non-official witness as well as the CBI have been of the view that the proposed Section should be recast to include 'child pornography' also and specific provisions should be incorporated in this Section to criminalize child pornography in tune with the laws prevailing in advanced democracies of the world as well as Article 9 of the Council of Europe Convention on Cyber Crimes which states as under:-

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
>
> (a) producing child pornography for the purpose of its distribution through a computer system;
>
> (b) offering or making available child pornography through a computer system;
>
> (c) distributing or transmitting child pornography through a computer system;
>
> (d) procuring child pornography through a computer system for oneself or for another person;
>
> (e) possessing child pornography in a computer system or on a computer-data storage medium.
>
> 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
>
> (a) a minor engaged in sexually explicit conduct;
>
> (b) a person appearing to be a minor engaged in sexually explicit conduct;
>
> (c) realistic images representing a minor engaged in sexually explicit conduct.
>
> 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may,

however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

120. When the Committee desired to hear the views of the Department of Information Technology in incorporating an express provision on defining child pornography as suggested by the Expert Committee, it was replied that a new Section 67 A related to punishment for publishing or transmitting of material containing sexually explicit acts has been proposed as per which stringent provision has been made relating to pornography in general and would also automatically cover child pornography.

121. On the issue of criminalising child pornography and making penal provision towards that, the Department stated that, the advice/assistance in the Commission of Crime (Pornography) through offering advice on information regarding the websites for facilitating any possession or downloading illegal content might be considered an offence.

122. The Department of Information Technology also agreed to a suggestion that the pre-offence grooming i.e. the initial actions taken by the offender to prepare the child for sexual relationships through online enticement and distributing or showing pornography to a child should also be made a criminal offence.

XII. Powers of Interception

(Clause 33)

123. Clause 33 of the Bill proposes to amend Section 69 of the principal Act which deals with the power to issue directions for interception or monitoring or decryption of any information through any computer resource. Such powers of interception are proposed to be vested with the Central Government and not with the State Governments.

124. In the above context, CBI and some other non-official witnesses were of the view that given the fact that 'Public Order' and 'Police' are State subjects as per Schedule VII of the Constitution and in view of the proliferation of cyber

crimes, it would be expedient to confer powers of interception on the State Governments also in tune with the provisions of the Indian Telegraphic Act, 1885.

125. They also suggested that interception should be allowed for prevention of any cognisable offence in addition to the prescribed grounds of sovereignty and integrity of India; security of State and defence of India; friendly relations with foreign States and public order. It has further been suggested that an emergency provision of interception, as provided in Section 5(2) of Indian Telegraph Act, 1885, should also be made in the IT Act, 2000.

126. Taking such views/suggestions into consideration, the Committee desired to be apprised of the comments of the Department of Information Technology. In reply it was stated that in case of computer to computer/internet communication the information can be accessed simultaneously from different points all over the country/world. In such a scenario, interception of information at one point will not prevent the access of such information from other points. For example, if a State Government takes a decision to block a site/information, it may be possible to do the same in a particular State whereas the information can be accessed from other States or other parts of the country. In such circumstances the very purpose of vesting power of interception in State Government will be defeated. The power of interception accordingly has been proposed to be vested with Central Government.

127. The Committee pointed out in evidence that the investigating agencies have invariably been working in the States as well. In such a scenario, the Committee desired to know, how would the State Governments be able to intercept e-mails without the powers to do so. Responding to the query of the Committee, a representative of the DIT stated that there were two issues involved i.e. one was blocking which had to be done at the national level at gateways and the other was interception which was done at the local level.

128. When it was made clear by the Committee that they were not interested in the first issue and categorically desired to know if an E-mail was to be intercepted in any State whether the concerned State Government was empowered to do so. In reply, another representative of DIT stated that there were five agencies which were authorised to do so. He further stated that such

interception was being done at the 'gateway' level and there was nothing called 'Central' level.

129. Asked to indicate the reasons for reluctance in incorporating provisions similar to Section 5 (2) of the Indian Telegraph Act, 1885 in order to empower the State Governments to intercept E-mails, the representative of DIT submitted:-

"For E-mails, today it is being done."

XIII. Traffic Data (Clause 36)

130. Clause 36 of the Bill intends to add a new Section 72 A which would make service providers and intermediaries liable for imprisonment upto two years and fine upto Rs. 5 lakh for disclosing personal information of their subscribers without the subscribers consent and with intent to cause injury or wrongful loss to the subscriber.

131. In this regard, the CBI while in general agreement with the provisions of this Section, suggested that specific provision should be made empowering the law enforcement agencies to call for information (subscriber and log data) from the service providers and others in the discharge of their official duties. They also suggested that the term 'traffic data may be defined to include subscriber and log data on the lines of Article 1 (d) of Council of Europe Convention on Cyber Crimes.

132. In the above context, the Committee desired to have the response of the Department of Information Technology. In reply it was stated that the word 'traffic data' has been used in "Convention of Cyber Crime" brought out by European Commission. The 'traffic data' is defined as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service". The term 'traffic data' requires careful examination. The online collection of data under the existing technological protocols IPv4 used for internet connectivity do not provide for such fields as defined in the definition of 'traffic data' directly. Any service provider needs to capture data online and process it further for arriving at 'traffic data' indicating the communication's

origin, destination, route, time, date, size, duration, or type of underlying service. It is an involving and requires a backend processing. Therefore, 'traffic data' cannot be stored online in real mode. It is, therefore, not recommended that word 'traffic data' is used in the Act.

XIV. Compounding Offences (Clause 37)

133. Clause 37 proposes to amend Section 77 and 78 of the principal Act by virtue of which the proposed Section 77 A will render offences under Sections 66, 66 A, 72 and 72 A compoundable.

134. The CBI suggested that offences under the above Sections should not be made compoundable as cyber crimes under the said Sections have been affecting the individuals besides causing irreparable damages to the security and economy of the country.

135. Asked to comment upon the above suggestion, the Department of Information Technology stated that compounding of offences under Section 66, 72, 72 A has been in line with the concept of "Plea-Bargaining" introduced recently by the Government. The compounding of contraventions has been proposed in order to facilitate litigants to settle disputes among themselves. This will lessen the burden on the courts and help in speedy settlement of disputes.

136. The Committee asked whether a concerted attempt was not being made to make offences less grave *vis-a-vis* the existing law, albeit with the purported intention of promoting the IT industry. In reply, it was stated that the provision of compounding offences would not apply where the accused, by reason of his previous conviction, was liable to either enhanced punishment or to a punishment of different kind for such offence.

XV. Powers to investigate and omission of Section 80 (Clauses 37 & 39)

137. Clause 37 of the Bill proposes to amend Section 78. As per this amendment, the power of investigation for a cognisable offence would rest with

an officer of the rank of a DSP and above. However, for investigations of a non-cognisable offence, a police officer of any rank can investigate but cannot arrest.

138. In the above context, the CBI submitted before the Committee that as there was a scarcity of DSP level officers in the field who were otherwise busy with law and order work, restricting the power of investigation of cognisable offences to DSP level officers would cause serious impediment in combating cyber crimes.

139. Echoing the same opinion, a retired Secretary (R&AW) while tendering evidence before the Committee stated:-

> ".....we feel that this provision which says that only DSP can investigate these cases goes against the spirit of treating all offences on the same footing. The Criminal Procedure Code has laid down a procedure for investigating cases. Even the murder case or a rape case is investigated by a Station House Officer. So, why IT cases cannot be investigated by him? We have a shortage of DSPs in the Police Force. I am told that the CBI's Cyber Wing has got only two DSPs and the Delhi Police has only one. The number of cases is going to be very large with the extension of IT culture. So, is there a need to confine the investigation of cognisable offences to the level of DSP?"

140. Clause 39 of the Bill seeks to omit Section 80 of the principal Act. Under the existing provisions of the said Section, an officer not below the rank of DSP is empowered to enter and search any public place and arrest without warrant any person found therein who is reasonably suspected of having committed or committing or about to commit any offence under the Act.

141. In this regard, the CBI and some non-official witnesses suggested that the existing Section 80 of the Act should be retained as there was a lot of preventive utility of the said Section, especially for search of cyber cafes widely used for communication by anti-national elements. One of the industry representatives was also of the view that it would make no sense to completely delete Section 80 of the Act.

142. The Ministry of Law and Justice (Legislative Department) when asked whether it was desirable to empower officers of the rank of DSP and above to investigate cognisable offences, stated that such a provision was desirable since investigation of most of the computer related offence needed a certain level of

technological knowledge that might not be available with all ranks of Police Officers.

143. The Committee then desired to know from the Department of Information Technology the rationale for empowering police officers of the rank of DSP and above to investigate cognisable offences under Section 78 as well as the logic for deletion of Section 80 of the principal Act. In reply, it was stated that the present Sections 78 and 80 were being proposed to be merged in order to classify offences rationally as cognisable and non-cognisable depending upon their severity and in line with the IPC. It was further stated that it was felt desirable to empower DSP level officers and above to investigate cognisable offences since investigation of such offences needed a certain level of technological knowledge that might not be available with all ranks which would likely result in unnecessary harassment of legitimate users.

144. Replying to a query of the Committee in this regard a representative of the DIT submitted during evidence that it was considered to be a little more matured approach to empower DSP level officers to investigate cognisable offences. The Committee asked whether it would be desirable to entrust the DSPs, who were mostly direct recruitees, with investigation of such complicated cases overlooking the vastly experienced Inspectors. In reply, the Secretary, DIT submitted:-

> "One is general knowledge about Information Technology. But in these cases, there has to be specialised knowledge, for instance, knowledge of cyber law."

145. The Secretary, DIT further stated that the Department believed that higher officers in the police hierarchy would better understand the nuances of cyber laws and in that context it was proposed that the DSP level officers be given the power to investigate cognisable offences.

146. Drawing the attention of the Department to a system evolved in Tamil Nadu since last three years whereby all the engineering colleges were to provide basic training courses in IT to all the lower level officers including the policemen, the Committee asked whether a similar system could be emulated nationwide in order to enable the officers of Inspector level to handle IT related cases efficiently. The Secretary, DIT replied:-

"We are thinking of doing training courses, as you said, as in-service training courses."

147. Referring to a note received from the Legislative Department wherein it was mentioned that the IT related registered cases nationwide rose from 68 in 2004 to 179 in 2005, the Committee pointed out that the enhanced penetration of internet and proliferation of IT into all sections of society and economy would invariably result in increased number of cyber offences. In this regard, the Committee asked whether it would not be prudent to impart training courses to lower level police officers for aptly handling the growing number of cyber crimes. In response, the representatives of the Department replied in the affirmative.

XVI. Miscellaneous

(a) Definition of computer network

148. Section 2(1) (j) of the IT Act, 2000 pertaining to the definition of 'computer network' reads as follows:.

"(j) "computer network" means the interconnection of one or more computers through -

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;"

Clause 4 of the Bill proposes to substitute the existing clause (j) as follows :-

"(j) "computer network" means the inter-connection of one or more computers or computer systems through-

(i) the use of satellite, microwave, terrestrial line, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more inter-connected computers whether or not the inter-connection is continuously maintained;";

(b) **Status of Indian Computer Emergency Response Team (CERT – In)**

149. The Department propose to add a new Section *viz.* Section 70A after Section 70 of the principal Act. The new Section reads as follows:-

"70A. (*1*). The Indian Computer Emergency Response Team (CERT-In) shall serve as the national nodal agency in respect of Critical Information Infrastructure for co-ordinating all actions relating to information security practices, procedures, guidelines, incident prevention, response and report.

(2). For the purposes of sub-section (*1*), the Director of the Indian Computer Emergency Response Team may call for information pertaining to cyber security from the service providers, intermediaries or any other person.

(3). Any person who fails to supply the information called for under sub-section (2), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(4). The Director of the Indian Computer Emergency Response Team may, by order, delegate his powers under this section to his one or more subordinate officers not below the rank of Deputy Secretary to the Government of India."

(c). Adjudication Process

150. Section 43 provides for civil remedy under which damages by way of compensation upto rupees one crore can be sought. But such compensation claims can be filed not before a court of law but before a statutory officer known as Adjudicating Officer.

151. In this context, the Committee were informed by some non-official witnesses that by an executive order in 2003, the Government have appointed

the IT Secretaries in each State as Adjudicating Officers and in the opinion of such witnesses the IT Secretaries have neither the time nor the inclination/professional ability to deal with such matters.

152. When the Committee desired to know the views of the Department of Information Technology on the above observations, it was replied that the executive order was issued by the Government for appointing Secretaries dealing with Information Technology in different States as Adjudicating Officers. This was done as Secretaries dealing with Information Technology in their respective States have knowledge of Information Technology and also have the necessary knowledge of the court processes as they have acted as Sub-Divisional Magistrates and District Magistrates. They have knowledge of Civil procedures, Code of Criminal Procedures and are in a position to provide a better citizen interface. The Adjudicating Officer in all the States were stated to be in place and no complaint of any nature in this regard was received in the Department.

153. During the course of the oral evidence a representative of the Department further clarified:-

> "Since Secretaries (IT) in different States are appointed as Adjudicating Officers, they are largely having engineering background. So, by an Executive Order Secretaries (IT) were appointed as Adjudicating Officers and they were given powers of Civil courts".

154. When asked to clarify as to whether the present arrangement of Secretary (IT) functioning as ex-officio Adjudicating Officer who has judicial/quasi-judicial powers was legally correct, the witnesses added:-

> ".....the Ministry of Law was consulted. Now the Cyber Appellate Tribunal is also in place. Justice R.C. Jain is functioning there. I had a discussion with him a couple of month ago. We requested him to study that and suggest if there are any changes to be made. Your suggestion is well taken and we will talk to him once again."

(d) Setting up of Special Courts

155. During the course of the examination of the Bill, the Committee were informed by some non-official witnesses that one of the main reasons for the IT Act remaining ineffective in its present form was the absence of Special Courts which could properly study and hear cases pertaining to the complicated cyber issues.

156. Commenting upon the above observation, the Department of Information Technology stated that the Adjudicating Officers with their day-to-day experience with matters pertaining to Information Technology were Special Courts in all practical purposes. It was further stated that all proceedings before the Adjudicating Officer were deemed to be judicial proceedings within the meaning of Section 193 and 228 of the Indian Penal code. The Adjudicating Officers have the powers of the civil courts and the proceedings would deem to be a civil court for the purposes of Section 345 and 346 of the Cr.P.C.

157. In the context of setting up of special courts to try cyber crime cases, the Ministry of Law and Justice (Legislative Department) stated that generally special courts were set up to relieve the burden of ordinary courts, provide for speedy trial and punishment for offences, deal with large number of cases of the similar nature or of peculiar nature and facilitate expeditious investigation of such nature of cases. They further stated that the number of cases registered under the IT Act, 2000 was very limited i.e. 60 cases in 2003, 68 cases in 2004 and 179 cases in 2005 as per the statistics available with the National Crime Records Bureau (Ministry of Home Affairs). The Legislative Department were, therefore, of the opinion that in view of the registration of limited number of cases under the IT Act, 2000, it would be appropriate if the cases continued to be tried by the ordinary courts.

(e) Spam

158. While examining the Information Technology (Amendment) Bill, 2006, the Committee were apprised by the industry representatives/legal experts that 'spam' or the issue of receiving unwanted and unwarranted e-mails have not been addressed under the proposed amendments.

159. In the above context, the Committee asked whether it would not be prudent to incorporate specific provisions in the proposed law to protect the e-mail account holders from unwarranted mails. In reply, the Department of Information Technology stated that Sub-Section (b) of Section 66 A and Clause (i) of Section 43 of the IT Act addressed the issues pertaining to spam.

160. As a close scrutiny of the above said two Sections revealed that the issue of spam had not been adequately covered, the Committee in evidence desired to

know how could the menace of spam be appropriately tackled with. In response, the Secretary, DIT replied that unwarranted e-mails could be generated from anywhere in the world.

(f) Powers of Controller of Certifying Authorities (CCA)

161. During the course of the examination of the Bill, suggestions were received from various quarters that instead of vesting the powers of 'Controller of Certifying Authorities (CCA)' vaguely in the Central Government which has been otherwise so hard pressed, some concrete safeguards should be found out.

162. Asked to comment on the above suggestion, the Department of Information Technology stated that Controller of Certifying Authorities had been assigned specific responsibility of licensing certifying authorities for issue of digital signatures and regulate the functioning of certifying authorities. Prescribing the best security practices and procedures was not part of his responsibilities in the principal Act. Central Government has been empowered to prescribe such security practices in the principal Act. A provision has been co-opted in Clause 20 and Central Government has been empowered accordingly. The Department further stated that the Clause 33 provided for substitution of new Section for Section 69 of the principal Act. The power to issue directions for interception or monitoring or decryption of any information through computer resources were being proposed to be provided to the Central government. The provisions have been in line with the guidelines laid down by the Hon'ble Supreme Court for interception of communication. The Department further stated that the subject of encryption, interception and decryption required input and coordination among different Ministries and Departments and it was, thus, felt that the Central Government would be in a better position to coordinate that rather than the Controller of Certifying Authorities.

163. When the Ministry of Law and Justice (Legislative Department) were asked to give their comments on the issue, they stated that there was no need to vest the powers of the Controller of Certifying Authorities (CCA) in the Central Government.

164. The Committee then asked the Department of Information Technology to respond to the above observation of the Legislative Department. In reply, it was stated that the powers of the CCA were limited to license the Certifying

Authorities and supervise their operation. Accordingly, Clause 12 has been proposed in the IT Bill to amend Section 29 of the IT Act where the powers of the Controller have been limited to the particular chapter only. The Department further stated that as the power of interception was a larger issue, the Central Government has been empowered to order for interception. However, to avoid single point choking the Central Government may provide the power to other agencies to deal with the cases in emergency situations.

165. In evidence, the Committee desired to know what constituted 'other agencies'. In reply, a representative of the Department stated that it was difficult to visualise which agencies would come into picture at what time due to technological requirements. The Secretary, DIT, supplementing his colleague stated:-

> "The present position is that it is being referred to the Department of Telecommunications. But tomorrow we may have a system where we have to require not only interception but also decryption. At the moment, the present position is regarding the blocking."

166. When the Committee desired to know the views of the Controller of Certifying Authorities on the above issue, he submitted in evidence:-

> "As per the present Act, any request for blocking comes to the Controller of Certifying Authority, and he examines it with the advice of the agencies concerned as to whether a particular site is to be blocked or not, or to be intercepted. Based on the inputs of the advice that is given, an order is passed. It is given to the Department of Telecommunications because they are the licensing agencies for all ISPs to take necessary action. That is the procedure which has been put and that procedure is being followed currently."

(g) Electronic Fund Transfer

167. The Committee, during the course of the examination of the IT (Amendment) Bill, 2006 received some suggestions from the industry representatives that there was a need for specific provisions in the law to legalise and enable electronic fund transfer. Similarly, the concept of electronic payments, digital cash, electronic cash, electronic money or other existing systems of electronic payments needed to be appropriately recognised.

168. In this regard, the Legislative Department also expressed the view that although electronic payment of money has been recognised by IT Act, 2000,

there was still a need for a separate Act for Electronic Fund Transfer since certain transactional issues could not be covered in the IT Act.

169. Asked to comment on the above suggestions, the Department of Information Technology stated that a separate Act for Electronic Fund Transfer needed to be drafted. Such an Act would address liability issues between sender, receiver of the funds and the service provider transmitting the funds. These are specialised issues and were not being covered in the IT Act and, therefore, a separate Act called "EFT Act" might be necessary. This approach was stated to have been adopted world wide. It was also stated that the Reserve Bank of India had been considering the formulation and legislation of such Electronic Fund Act.

170. The Committee, during the oral evidence, desired to be apprised of the latest position in this regard. In response, a representative of the Department stated:-

> ".....we checked it up with the RBI with respect to the latest details of Electronic Transfer Act. What they have said in writing is that the Payment and Settlement System Bill is coming up for approval in the next Parliament.Session. Standing Committee have already given its recommendations on this Bill. This Bill is comprehensive. As such, no other separate Act will be necessary for payment system. What it primarily means is the Payment and Settlement Bill takes care of this element."

RECOMMENDATIONS/OBSERVATIONS

Introductory

1. The Committee note that the Information Technology Act was enacted in the year 2000 and implemented with effect from 17 October, 2000. The Act which consists of 94 Sections and 4 Schedules was meant to provide a legal framework for promotion of e-commerce and e-transactions and also give a fillip to growth and usage of computers, software, internet, etc. The Act was also enacted with a view to legalising evidentiary value of electronic record and computer/cyber crimes which are of technical nature. However, like any other technology driven law, the Act acquired obsolescence and therefore a need was felt to amend it within six years of its enactment primarily due to proliferation of IT into various walks of life, phenomenal growth in outsourcing business, new means of transactions and identifications, emergence of newer forms of misuse of computers etc. Therefore, an Expert Committee headed by the Secretary, Department of Information Technology, Government of India was set up in January, 2005 in order to make the Act technology neutral, to co-opt various provisions for data protection and to update the Act as per changing scenario. The Expert Committee submitted their Report in August, 2005. Based on the recommendations of the Expert Committee, the Government have sought to make changes in the IT Act through amendments to the existing legislation. Thus, the Information Technology (Amendment) Bill, 2006 was introduced in Parliament on 15.12.2006 and referred to this Committee for detailed examination and report.

Self enabling and people friendly laws

2. The IT Act, 2000 draws sustenance in respect of several provisions from various sources like the Indian Penal Code (IPC), 1860, the Criminal Penal Code (Cr. P.C.), the Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891, Reserve Bank of India Act, 1934 etc. To-day, information technology has reduced the world to a global village. The law pertaining to IT should, therefore, be self containing and easily comprehensible to the global village community. The Committee, however, regret to note that the Government have not acknowledged this underlying principle despite the experience gained in about seven years in the administration of the IT Law and no effort has been made to bring a new and exclusive legislation. What has been attempted is to go for a 'short cut route' by making certain changes in the existing legislation and the other relied upon Acts. Justifying this, the representatives of DIT have maintained that the experts who were engaged while drafting the Bill have been of the opinion that IPC and Cr.P.C. from which the principal Act of 2000 draws sustenance in respect of several provisions, have stood the test of time. The Committee feel that to the extent of their local applicability they are very appropriately worded in the primary and basic Acts. However, when laws pertaining to information technology are taken into consideration, then the connotations change drastically. The Committee are of the view that the IT laws for their universal application, should be self-enabling and comprehensive so that a mere reading of the relevant clause is sufficient for any agency/individual concerned sitting anywhere in the world to comprehend the import and culpability. The Committee consider it unfortunate that the Government did not choose to bring a new and

exclusive Bill in order to make the IT Law very comprehensive, self enabling and people friendly which undoubtedly would have been more effective in enforcement.

Cyber Crime and Cyber Terrorism

3. During the course of the examination of the IT (Amendment) Bill, 2006, the Committee's attention was drawn towards inadequate focus on and coverage of cyber crime including cyber terrorism in the proposed law. The Committee are really surprised to observe that the term 'cyber terrorism' has not been defined anywhere in the IT Act, 2000 or in the proposed amendments. The Department's statement that it may be considered to incorporate provisions to make cyber terrorism a punishable crime with highest fine and imprisonment in line with Sections 120 B and 121 of IPC does not impress the Committee as the centuries old Indian Penal Code may not be all encompassing to include different types of emerging cyber crimes including cyber terrorism. Moreover, in view of the fact that cyber crimes intend to create havoc and destablise the society and cyber terrorism is equivalent to waging war against the nation, the Committee strongly recommend that adequate, stringent, specific and self enabling provisions should be incorporated in the IT Act itself to deal with such offences.

Jurisdiction of Law

4. Another disquieting aspect that has come to the notice of the Committee relates to the jurisdiction and applicability of the Act for dealing with cyber offences committed outside India. This aspect is presently included in Section 1(2) and Section 75 of the IT Act, 2000.

The Committee's examination revealed that the provisions contained in these two Sections in their present form seem to be inadequate for the Country to enforce its will in cases where cyber crimes are committed against India from outside the geographical boundaries of the Country. During examination this disturbing inadequacy was candidly admitted by various stakeholders including legal experts, industry representatives, Central Bureau of Investigation (CBI), Legislative Department and the Department of Information Technology (DIT). However, the Committee have been informed by the official witnesses during evidence that Sections 3 and 4 of the Indian Penal Code (IPC), if interpreted properly, have enough scope and can cover wider areas. It has also been informed that the Government have signed Mutual Legal Assistance Treaties (MLATs) with 17 countries till date which will cover cyber crimes. Further, similar Treaties with nine other countries have been stated to be under process. The Committee cannot remain contented with this. After examining the issue in its wider implications, the Committee are of the view that the relevant general laws in the IPC are time consuming procedures and hence not sufficient to deal with situations of cyber crimes committed against the country from foreign locations. The cyber crimes committed in virtual space have no boundaries and therefore, the legal framework to tackle such confine less incidents ought to be so suitably modified that the impediments of regions/geographical boundaries are not taken advantage of to delay or deny justice. Moreover, the cyber crimes including cyber terrorism are wanton acts committed in split second from remote places and hence they require to be tackled with the same speed and a justice delivery system that is as quick. Therefore, instead of taking recourse to piecemeal solution of

entering into MLATs with one country at a time, the Committee would prefer that India should be a signatory to an omnibus International Convention on the issue so that cyber crimes committed against any country from anywhere are tackled with utmost promptitude and without the technicalities of citizenship, etc. coming into play. The Committee, therefore, strongly feel that India as one of the world leaders in information technology, ought to take initiative in materialising such an International Convention against cyber crimes/cyber terrorism under the auspices of United Nations. Accordingly, they desire that the Department should immediately prepare a roadmap in consultation/coordination with the Ministries of External Affairs, Law and Justice and Home Affairs for a suitable international Convention. The Government may, in the meantime, utilize their diplomatic channels for creating a movement in favour of the Convention in the comity of nations. The Committee are hopeful that such an initiative by the Government of India under the auspices of United Nations will tackle the twin scourge of cyber crimes and cyber terrorism to a substantial extent universally and spare the Government from taking recourse to adhoc approaches/arrangements to counter a perennial problem. The Committee would like to be apprised of the initiatives taken in this matter.

Substitution of 'digital signature' by 'electronic signature'.

(Clause 2)

5. The Committee note that pursuant to a resolution passed by the United Nations in the year 2001 recommending that all the States should give favourable consideration to the Model Law on 'Electronic Signatures' when enacting or revising their laws, the Information

Technology (Amendment) Bill, 2006 *vide* Clause 2 proposes to substitute the words 'digital signature', wherever occurring in the principal Act, by the words 'electronic signature'. The Committee also find that ' digital signature', in fact, is one of the types of 'electronic signature' and is considered to be one of the most reliable methods for security, integrity and authentication of electronic records. However, in view of the difficulty to amend the Act very frequently and keeping in mind the ever-evolving technological developments, a need has been felt to substitute 'digital signature' by the all encompassing term 'electronic signature'. The Committee feel that it is a step in right direction to put emphasis on reliable electronic signature as it would enable the Central Government to take steps commensurate with the needs of emerging technologies. Although some mechanism has been stated to be put in place to guard against forgery of digital signature, yet the Committee desire that in view of the immense importance of being a better alternative to paper based methods of communication and storage of information, awareness programmes should be resorted to in association with the industry to educate the citizens on the possible misuse/abuse of digital signature.

6. The Committee also desire that in order to facilitate implementation of the ambitious National e-Governance Plan (NEGP) with active public participation, the Department should make earnest endeavors to make digital records available to the general public in people friendly and easily accessible formats. In view of the extant socio-economic milieu, the Committee desire that the affordability factor should be taken into consideration while making digital records available to the common man.

Auditing of Electronic Records

7. The Committee note that according to the representatives of the industry auditing of electronic records is desirable as per the global practice to provide some legal sanctity to these records and check frauds that are constantly occurring in corporate India. The DIT, while concurring with the appropriateness of the suggestion, have regrettably passed on the onus to the industry to find out more details regarding the global practices and standards in this regard. The Committee disapprove such an attitude of the nodal Department as they themselves should have done all the spade work in this regard. However, after interaction with the industry representatives, the Committee feel that auditing of electronic records is a pressing need in the present scenario when more and more data and records are not only being generated digitally but even the existing ones are being digitalised for excellent retention value and easy storage and retrieval. During the course of the examination, the Committee could comprehend that even DIT are not fully clear about the status of digitally generated records, albeit they being official government documents. The Committee, therefore, desire that a suitable clause be inserted in the Bill to make auditing of electronic records mandatory so that electronic records both in terms of information system and information security are accorded clarity, authenticity and legal sanctity.

Definition and role of Intermediary and liability of network service providers

(Clause 4 and Clause 38)

8. Section 2 (w) of the IT Act defines 'intermediary' with respect to any particular message as any person who on behalf of any other person receives, stores or transmits that message or provide any service with respect to that message. The Committee note that Clause 4 sub-clause (F) of the Bill now seeks to define the term 'intermediary' as any person who on behalf of another person receives, stores or transmits electronic records or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes. It also seeks to explicitly exclude 'body corporate' as referred to in Section 43 A of the principal Act as an intermediary. The Committee also find that Clause 38 of the Bill proposes to substitute the entire Chapter XII of the principal Act whereby the intermediaries are absolved of liability in certain cases. In some other situations, the culpability of the intermediaries has been fixed. To exercise further control over the intermediaries, Clause 38 also stipulates that they shall observe such other guidelines as the Central Government may prescribe in the matter under sub-section 4 of Section 79. After carefully going through the various proposals, the Committee are constrained to point out that the definition and role of intermediaries sought to be made through the amendments are not very clear, particularly with regard to the exclusion of body corporate referred to in Section 43 (A) of the Bill. They, therefore, desire that the Department should reexamine Clause 4

(F) of the Bill so that there is no scope for ambiguity while interpreting the definition and role of the intermediaries.

9. The Committee observe that under the existing provision of the IT Act, 2000 the network service providers are made liable for all third party content or data. But under the proposed amendments, the intermediaries/service providers shall not be liable for any third party information data, or communication link made available by him, except when it is proved that they have conspired or abetted in the commission of the unlawful act. The Department's reasoning for not making the intermediaries/service providers liable in certain cases is that a general consensus was arrived at, while discussions were going on the amendments to the IT Act, to the effect that the intermediary/service providers may not be knowing what their subscribers are doing and hence they should not be penalised. The Committee do not agree with this. What is relevant here is that when their platform is abused for transmission of allegedly obscene and objectionable contents, the intermediaries/service providers should not be absolved of responsibility. The Committee, therefore, recommend that a definite obligation should be cast upon the intermediaries/service providers in view of the immense and irreparable damages caused to the victims through reckless activities that are undertaken in the cyber space by using the service providers' platform. Casting such an obligation seems imperative, more so when it is very difficult to establish conspiracy or abetment on the part of the intermediaries/service providers, as also conceded by the Department.

10. What has caused further concern to the Committee, in the above context, is that the Bill proposes to delete the words 'due diligence' as has been existing in Section 79 of the principal Act. The Department's logic for the proposed removal of the words 'due diligence' is the intention to explicitly define the provisions under Section 79 pertaining to exemption from liability of network service providers. The Department have further contended that the words 'due diligence' would be covered under the guidelines which the Central Government can issue under sub-section 4 of Section 79 of the principal Act. The Committee do not accept the reasoning of the Department as they feel that removing an enabling provision which already exists in the principal Act and leaving it to be taken care of by the possible guidelines makes no sense. They are in agreement with the opinion of some of the investigating agencies that absence of any obligation to exercise 'due diligence' would place some of the intermediaries like online auction sites/market places in an uncalled for privileged position thereby disturbing the equilibrium with similar entities that exist in the offline world. The Committee also feel that if the intermediaries can block / eliminate the alleged objectionable and obscene contents with the help of technical mechanisms like filters and inbuilt storage intelligence, then they should invariably do it. The Committee are of the firm opinion that if explicit provisions about blocking of objectionable material/information through various means are not codified, expecting self-regulation from the intermediaries, who basically work for commercial gains, will just remain a pipedream. The Committee, therefore, recommend that the words 'due diligence' should be reinstated and made a pre-requisite for

giving immunity to intermediaries like online market places and online auction sites.

Contraventions of serious nature

(Clause 19)

11. Section 43 of the IT Act, 2000 provides for payment of compensation not exceeding rupees one crore as penalty for damages to computer, computer system, etc. It enlists eight situations under Clauses (a) to (h) where the damages are liable to be paid. The Committee note that the amending Bill proposes that the marginal heading of Section 43 be changed from 'Penalty' to 'Compensation'. An additional Clause [(i)] relating to destruction/alteration, etc. of information in a computer resource has also been added. While agreeing with the additional Clause, the Committee tend to share the apprehensions of some of the investigating agencies regarding gravity of contraventions enumerated in Clauses (c) to (i). These contraventions are of serious nature and may have calamitous consequences in many cases, more so where Intellectual Property Right (IPR) or related aspects and security matters are involved. They, therefore, feel that merely a compensation not exceeding one crore rupees may not suffice. The Committee, therefore, desire that Clauses (c) to (i) of Section 43 be made cognizable offences punishable with three years imprisonment and fine. Furthermore, the contraventions under Clauses (c) to (i) ought to invite a fine substantially greater than one crore rupees as a detriment. In any case, the quantum of fine is qualified by the word 'not exceeding'. As regards contraventions under Clauses (a) and (b) the extant compensation may be retained. The side

heading of amended Clause 43 may, therefore, be retained as in the principal Act.

Compensation for failure to protect data

(Clause – 20)

12. The Committee note that under the proposed new Section 43 A, obligation is cast upon 'body corporate' for paying damages through compensation. The industry representatives are of the view that the obligation to pay damages by way of compensation should also extend to any person operating the information alongwith the body corporate owning or controlling personal information. According to the Department, the issue was extensively debated by the Expert Committee in consultation with industry representatives like NASSCOM and then it was decided to restrict the Section to body corporates alone. The Committee appreciating the position recommend that the obligation of paying damage through compensation for the time being be restricted to body corporate only. Extension of the Section to individuals may be considered once the system is put in place and experience gained.

13. The Committee observe that Clause 20 of the Bill proposes to insert a new Section 43 A which provides to impose a fine not exceeding Rs. 5 crore upon body corporates in case of being negligent in implementing and maintaining reasonable security practices and procedures. The Committee also note that initially an amount of Rs. 25 crore was suggested as fine, but upon the insistence of the industry it was decreased to Rs. 5 crore. According to the industry, Rs. 5 crore as prescribed under the law, is a sufficient deterrent because certainty of

punishment and not necessarily the extent is what matters. The industry have further submitted that the Courts of Law generally give the benefit of doubt to the defendant in severe punishment cases where evidence is not completely fool proof. The Committee are in absolute disagreement with the views expressed by the industry in suggesting the fine at Rs. 5 crore. They feel that on the plea of certainty of punishment, the extent of fine should not be on such a lower side. Moreover, the Court judgements are perceivably based on fool proof evidences, irrespective of the severity of cases. The Committee, therefore, urge upon the Department to restore at least the originally suggested amount of Rs. 25 crore as damages by way of compensation to be imposed upon the body corporates for negligence in implementing and maintaining reasonable security practices and procedures. The Committee are hopeful that such an increase commensurate with the magnitude of the IT industry, will send a right message to the stakeholders across the globe.

14. The Committee also find that as per the existing mechanism for imposition of the damage of rupees five crore, the victim has to go to the Adjudicator, then to the Cyber Tribunal and as a last resort to the High Court and the Supreme Court. The Committee feel that it is too cumbersome a procedure which has been corroborated by the industry when they have stated that in not a single case in the last several years even one rupee damage by way of compensation has been awarded in India. The Committee, therefore, desire that the Department should initiate action in consultation with other appropriate agencies to simplify the complicated adjudication process so that the remedy of providing damages by way of compensation is effectively implemented.

15. The Committee observe that as of now there is no specific provision in the Bill for protection and retention of data as agreed to by the industry, investigating agencies, legal experts and the Legislative Department, albeit the principal Act draws sustenance in this regard from other enabling laws. In the opinion of the Committee, it is but essential that there should be clear-cut and specific provisions for data protection and retention in the amended Act as the retention of accurately recorded, protected and retrievable research data is of utmost important for facilitating scientific integrity and investigations.

16. The Committee also feel that specific provisions prescribing suitable punitive measures for the recipient of stolen data need to be incorporated in this Section. This is one field where the intentions of the recipient are not above board in most of the cases and hence the culpability aspect cannot be overlooked or ignored.

17. As regards the issue of personal privacy, the Committee are not convinced by the logic extended by DIT about non-inclusion of specific provisions in this regard in the Bill as the issue requires a wider debate. Ideally, the Committee would have preferred the inclusion of this important aspect in the draft Bill itself, however, this was not done. Now that the Department have veered towards the view taken by the Committee, they would like the Department to add suitable provisions to define and protect personal privacy.

18. The Committee further note that, according to the explanation of the Department, the terms wrongful loss and wrongful gain are being co-opted in the Bill in tune with the IPC where these words are well defined. At the cost of appearing repetitive, the Committee would like to

impress upon the Department that in order to make the new law a more comprehensive and user friendly one, these terms ought to be defined unambiguously and definitely in the context of information technology/cyber related matters/contraventions.

Powers to Civil Courts

(Clause 29)

19. The Committee note that according to Section 61 of the principal Act, 'no Court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.' However, Clause 29 of the Bill proposes to amend the above Section by saying 'Provided that the Court may exercise jurisdiction in any cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter.' In the above context, the industry representatives have opined that the circumstances under which the Civil Court's role will come into play should be clarified. They have further suggested that it should also be clarified whether the Civil Court could restrict the jurisdiction of the Tribunal in the present case. The Department's response that it will be appropriate for the Adjudicating Officer to transfer the cases, where the damages claimed exceed the maximum prescribed amount, to an appropriate Court does not seem to appropriately address the concerns of the industry. The Committee find sufficient justifications in the points

raised by the industry representatives and desire that the circumstances under which the Civil Courts role will come into play should be spelt out clearly and it should also be clarified whether the Civil Court can restrict the jurisdiction of the Tribunal in the instant case. Utmost care should, however, be exercised while clarifying/modifying the existing Section lest the alleged offenders misuse such an enabling Clause to circumvent the jurisdiction and authority of the Adjudicating Officer in these matters.

Quantum of Punishment

[(Clauses 31, 36, 37, 49 (e), 49 (h) and 51 (a)]

20. The Committee observe that Clause 31 of the Bill proposes to amend sections 66, 67 & 67 A whereby the quantum of punishment for cyber crimes will be reduced to two years and thereby making such offences non-cognisable. Similarly, Clause 36 of the Bill proposes to insert a new Section 72 A where again, offences will be made non-cognisable. The Committee further note that Clause 37 intends to substitute Section 77 & 78 of the principal Act by new Sections 77, 77 (A), 77 (B) and 78. As per the proposed Section 77 (A), offences committed under Sections 66, 66 A, 72 and 72 A will be made complaint offences. *Vide* Clause 49 (e) of the Bill, Section 417 A is proposed to be incorporated in the IPC to criminalise cheating by use of the electronic signatures and password, etc. Here also, this offence is proposed to be made non-cognisable. Likewise, *vide* Clause 49 (h) of the Bill, a new Section *viz.* Section 502 A of the principal Act is proposed to be incorporated in the IPC to criminalise invasion of privacy by imaging and transmission of private parts of someone. This offence is proposed to be made non-cognisable. Moreover, Clause 51 (a) of the Bill proposes

to add a new Section 98 D in Cr.P.C. vide which no court shall take cognizance of an offence punishable under Sections 417 A, 419 A and 502 of IPC except on complaint of the aggrieved. However, offences under Section 419 A only are proposed to be made cognisable. Thus, the various amendment proposals seek to tone down the quantum of punishment for various types of cyber crimes. Expressing their serious reservations on this, the Central Bureau of Investigation (CBI) and some industry representatives have maintained that in view of their gravity, offences under all the above cited Sections should be made cognisable. On the other hand, the Department of Information Technology have stated that these punishments are proposed to be rationalised because while penal provisions are necessary to prevent flagrant abuse of the system, care has to be taken that such provisions do not give occasion for harassment of legitimate users and the common man ignorant of the nuances of information technology. In a nutshell, the Department's contention is that since people are not getting bails easily, they propose to keep offences under the above Sections non-cognisable. The Committee are astonished by such a reasoning. They are of the opinion that facilitation of bail to the alleged offenders of cyber crimes cannot and should not be construed a valid reason for reducing the quantum of punishment and thereby making it non-cognisable. Similarly, it is hard to believe that the alleged offenders are not aware of the nuances of information technology and in any case ignorance can not be an excuse for perpetrating crimes. As cyber crimes are a global phenomenon taking place with lightning speed, unmindful of the adverse ramifications upon all sections of the society, the Committee urge upon

the Department to initiate immediate measures to make cyber offences under all the above said Sections cognisable.

21. The Committee are surprised to note the statement of the Department of Information Technology that according to the Law Ministry, Schedule II of the Cr.P.C. is not amendable to incorporate a provision for making imprisonment of three years bailable. The Committee desire that the Department of Information Technology and the Ministry of Law and Justice should work out modalities to examine whether making imprisonment of three years bailable will be in the best interest of the nation and help the Government to encourage enhanced usage of computer/internet and proliferation of e-Governance and Information Technology for better productivity.

Definition of the terms 'dishonestly' and 'fraudulently'

(Clause 31)

22. The Committee observe that Clause 31 of the Bill explains that the words 'dishonestly' and 'fraudulently' shall have the same meaning as assigned in Sections 24 and 25 respectively of the Indian Penal Code. According to the Department of Information Technology, the existing definitions of these two terms in IPC are proposed to be used in the IT Act as both the terms are being used in reference to the crime and the Courts very well understand interpretations of these definitions. According to the Ministry of Law and Justice (Legislative Department), the two terms as appearing in the IPC should be incorporated in the IT Act in order to avoid any confusion as well as different interpretations by different Courts in the country. The Committee feel that the said terms may be different while dealing with cyber offences from what is

ordinarily understood in the general penal law of the country. Going by the statement of the Department of Information Technology and Legislative Department that the Courts very well understand the definitions of the two terms as defined in the IPC, the Committee are inclined to believe that the Courts will equally understand the two terms if defined separately in the IT Act with reference to the cyber crimes committed. The Committee, therefore, desire that the Department should examine the matter in all its implications for formulating appropriate definitions of the expressions 'dishonestly' and 'fraudulently' in the IT Act. The Committee may be apprised of the decision arrived at in this regard expeditiously.

Omission of the word 'hacking'

23. The Committee note that Clause 31, while intending to amend Section 66 proposes to delete the word 'hacking'. In this regard, a number of views have been received pointing out absence of logical rationale in deleting the offence of hacking under Section 66 of the existing law as the current provisions of that Section of the principal Act are very wide to fight newly emerging kinds of cyber crimes. According to the Department, hacking is more a colloquial word and will change over a period of time and although the word 'hacking' is proposed to be removed, yet all the features of hacking have been adequately covered in Clause 19 of Section 43 and Clause 31 of Section 66. The Department have further submitted that Section 43 A is more of a civil kind whereas hacking as appeared in Section 66 is a criminal offence and in their effort to avoid seamless mapping in both the Sections the word 'hacking' is proposed to be removed. The Committee find no justification in such

arguments in deleting the word 'hacking' as it existed in the principal Act. The Committee feel that hacking under Section 66 of the IT Act is one provision that is applicable to and is available with the law enforcement agencies across the country for booking all kinds of new cyber crimes. Therefore, as the proposed deletion of hacking will adversely affect the capability of the law enforcing agencies/officers to bring to book the cyber offenders, the Committee are of the strong opinion that 'hacking' should be retained in its original form. The Committee are confident that retaining the existing language of Section 66 of the IT Act and making hacking an offence under the Indian Cyber Law will send a right message to the stakeholders globally.

Child Pornography

24. The Committee note that Clause 31 of the Bill intends to insert a new Section 67 A which provides for stringent punishment for publishing or transmitting of material containing sexually explicit acts in electronic form. But the Committee are concerned to find that the term 'child pornography' has nowhere been mentioned in the proposed Section. The Department's argument that the Section while covering 'pornography' will automatically cover child pornography does not convince the Committee as there should be no scope for assumption or presumption when fresh amendments are being proposed. The Committee, therefore, impress upon the Department to include the term 'child pornography' in the proposed Section 67 A in view of its growing menace. They also desire that specific provisions should be incorporated in this Section to criminalise child pornography in tune with the laws prevailing in the advanced Countries and Article 9 of the

Council of Europe Convention on Cyber Crimes. In view of the several manifestations of sexual abuse of the children and its loathsome ramifications, the Committee desire that the act of grooming the child for sexual relationship through online enticement or distributing/showing pornography or through any online means should also be made a criminal offence and a suitable provision be made in this regard in the proposed Section 67 A.

Powers of interception

(Clause 33)

25. The Committee observe that Clause 33 of the Bill proposes to amend Section 69 of the principal Act which deals with the power to issue directions for interception or monitoring or decryption of any information through any computer resource. The Committee also note that such powers of interception are proposed to be vested with the Central Government and not with the State Governments. The rationale for not conferring powers of interception on the State Governments, according to the Department, is that if a State Government takes a decision to block a particular site/information, it may be possible to do so in that State, but such information can be accessed from other States or other parts of the country, thereby defeating the very purpose of vesting powers of interception in the State Governments. The Committee are not satisfied with the reasoning, because blocking and interception are two very different things. They understand blocking of information at one point will not prevent the access of such information from other points, as cyber information passes through national and regional gateways. The Department's statement that at present interception is

being done at the 'gateway' level and there is nothing called 'Central' level does not impress the Committee. Taking all the above factors into account and in view of the fact that 'Public Order' and 'Police' are State subjects as per Schedule VII of the Constitution, the Committee feel 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. The Committee also desire that an emergency provision of interception, as provided in the said Section of the Indian Telegraph Act, 1885 should be incorporated in the IT Act to combat proliferation of cyber crimes. In view of the emerging kind of cyber offences, the Committee further recommend that interception should be allowed for prevention of any cognisable offence in addition to the already prescribed grounds of sovereignty and integrity of India; security of State and defence of India; friendly relations with foreign States and public order.

Traffic Data
(Clause 36)

26. The Committee note that Clause 36 of the Bill proposes to add a new Section 72 A which will make service providers and intermediaries liable for imprisonment upto two years and fine upto Rs. 5 lakh for disclosing personal information of their subscribers without the subscriber's consent and with the intent to cause injury or wrongful loss to the subscriber. Commenting on this proposal, the Central Bureau of Investigation (CBI) have stated before the Committee that specific provisions should be made empowering the law enforcement agencies to call for information (subscriber and log data) from the service providers

and others in discharge of their official functions. They are also of the opinion that the term 'traffic data' should be defined to include subscriber and log data in tune with the Article 1 (d) of Council of Europe Convention on Cyber Crimes. However, the Department of Information Technology are not in favour of incorporating and using the term 'traffic data' in the Act on the ground that it is an involving task and requires a careful examination as a service provider needs to capture data online and process it further for arriving at 'traffic data' indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service. The Committee are surprised to observe the logic of the Department for not including the term 'traffic data' in the Act. They feel that with the resources and expertise that are at the disposal of the Department, they should involve themselves and carefully examine the feasibility of incorporating and using the term 'traffic data' in the Act and also defining it appropriately to include subscriber and log data for facilitation of investigations by the law enforcement agencies. In the opinion of the Committee, the law ought to be crystal clear to the maximum extent so that the enforcement agencies are clear in their mind about how to proceed against offenders so that the legal proceedings in cyber crimes do not get mired into unnecessary controversies, thereby delaying justice.

Compounding Offences

(Clause 37)

27. The Committee observe that Clause 37 of the IT (Amendment) Bill, 2006 proposes to amend Sections 77 and 78 of the principal Act as a result of which the proposed Section 77 A will render offences under

Sections 66, 66 A, 72 and 72 A compoundable. According to the Central Bureau of Investigation (CBI), offences under the above Sections should not be made compoundable as cyber crimes under the said Sections are affecting the individuals beside causing irreparable damages to the security and the economy of the country. According to the Department of Information Technology, the compounding of contraventions are proposed in order to facilitate litigants to settle disputes among themselves and speedy settlement of disputes. The Department have, however, further submitted that the provision of compounding offences will not apply where the accused, by reason of his previous conviction, is liable to either enhanced punishment or to a punishment of different kind for such offence. Thus their contention seems to be that serious offences cannot be compounded. However, keeping in view the concerns expressed by the premier investigating agency, the Committee desire that the situations where compounding of offences will not be applicable should be unambiguously spelt out in the Bill to put to rest any apprehensions in this regard.

Powers to investigate and omission of Section 80

(Clauses 37 & 39)

28. The Committee note that Clause 37 of the Bill proposes to amend Section 78 of the principal Act by virtue of which the power of investigation for a cognisable offence will rest with an officer of and above the rank of a Deputy Superintendent of Police (DSP), though the responsibility for investigation of a non-cognisable offence is vested with a police officer of any rank without the power to arrest. According to the Department of Information Technology and the Ministry of Law

and Justice (Legislative Department), such a provision of empowering atleast a DSP rank officer to investigate cognisable offences has been made on the ground that investigation of offences like cyber crimes need a certain level of technological knowledge that may not be available with all ranks of police officers. Moreover, the Government consider it a matured approach to empower DSP level officers to investigate cognisable offences. The Committee are unable to accept such reasoning as they are of the view that when Station House Officers can investigate much sensitive cases like murder and rape, there is no point in confining investigation of IT related cases to DSP and above rank officers, especially in view of their scarcity and other pressing assignments. Moreover, the general perception that only DSP and above rank police officers can better understand the nuances of information technology does not impress the Committee in view of the fact that now-a-days given the current educational system and avenues available all around, every graduate/post graduate has a passion to acquaint herself /himself with information technology. In view of the above and taking into consideration the fact that the penetration of internet and proliferation of IT into all sections of society and economy has resulted in increased number of cyber offences, as has been corroborated from the figures furnished by the Ministry of Law and Justice (Legislative Department), the Committee recommend that investigation of cognisable cyber offences should be entrusted with the officers of Inspector level and above.

29. The Committee are also given to understand that some State Governments like Tamil Nadu have asked all the Engineering Colleges in the State to provide basic training course in IT to all personnel in their

police forces. This step would certainly help these trained officers to efficiently deal with IT related cases. The Committee desire that the Department of Information Technology in consultation with the Ministry of Home Affairs should take immediate initiatives to convince other States to emulate the practice resorted to by the Tamil Nadu Government in imparting basic training courses to police personnel and others so that the Inspector level officers are adequately trained to handle cyber crime cases.

30. The Committee observe that Clause 39 of the Bill seeks to omit Section 80 of the principal Act under the provisions of which an officer not below the rank of DSP is empowered to enter and search any public place and arrest without warrant any person found therein who is reasonably suspected of having committed or committing or about to commit any offence under the Act. According to the CBI and the industry, the existing Section 80 of the Act should not be deleted altogether as there is lot of preventive utility of the said Section, especially for search of cyber cafes widely used for communication by anti-national elements. The Department's contention in proposing to delete the said Section is to merge Sections 78 and 80 in order to classify offences rationally as cognisable and non-cognisable depending upon their severity and in line with the Indian Penal Code. The Committee are not inclined to accept the views expressed by the Department for proposing to delete Section 80 as such an act will prove detrimental to the society and national interest for it will seriously impair the power of searching and raiding cyber cafes widely perceived as being misused as havens for anti-social and anti-national elements. The Committee, therefore, recommend that Section 80 of the principal

Act should be retained with some modifications commensurate with the suggestions of the Committee for Section 78.

Miscellaneous

(a) Definition of computer network

31. The Committee note that Clause 4 of the Bill proposes to amend section 2 (1) (j) of the principal Act by adding the word 'wireless' in order to amplify the definition of 'computer network'. The Committee while appreciating the move, desire that the word 'wired' may also be included between the words 'terrestrial line' and 'wireless' to give more clarity to the Clause.

(b) Status of the Indian Computer Emergency Response Team (CERT-In)

32. The Committee note that the Department have proposed a new Section *viz.* 70A to notify the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency. However, the status of CERT-In has not been defined in the proposed Section. The Committee, therefore, desire that the words 'a Government body' may be inserted in the new section in sub-section 70A(1) immediately after the words 'The Indian Computer Emergency Response Team (CERT-In)', to clarify the status of the body beyond any doubt. In the view of the Committee, this would not only make the definition of CERT-In more clear but also, as the Department have time and again emphasised, will instill confidence in the foreign investors regarding existence of a bonafide legal frame work in the Country.

(c) Adjudication Process

33. The Committee note that Section 43 provides for civil remedy under which damages by way of compensation upto rupees one crore can be sought. But such compensation claims can be filed not before a court of law but before a statutory officer known as Adjudicating Officer. The Committee find that by an executive order in 2003, the Government have appointed the IT Secretaries in each State as Adjudicating Officer. In this context, some non-official witnesses, who deposed before the Committee, are of the opinion that IT Secretaries have neither the time nor the inclination and professional ability to deal with such matters. But according to the Department, the IT Secretaries have adequate knowledge of civil and criminal procedures and matters relating to information technology and thus they are in a position to provide a better citizen interface. The Department have further submitted that such an arrangement is made on the pattern of the SEBI Act and no complaint of any nature has been received in this regard. Even then, taking into consideration the concerns expressed in this regard, the Department have requested the Ministry of Law and Justice and the Cyber Appellate Tribunal to study and suggest whether any change is required in the process of appointment of Adjudicating Officers. Appreciating the step taken by the Department to address the above mentioned concern, the Committee would like to be apprised of the opinion of the Ministry of Law and Justice as soon as the review on the matter is complete.

(d) Setting up of Special Courts

34. In the process of the examination of the Bill, the Committee have been given to understand by some industry representatives that one of the main reasons for the IT Act remaining ineffective in its present form is the absence of Special Courts which can properly study and hear cases pertaining to the complicated cyber issues. But the Department are of the view that the Adjudicating Officers with their day-to-day experience and efficient dealing with matters pertaining to information technology are Special Courts for all practical purposes and hence there is no need to set up Special Courts to try cases relating to cyber crimes. The Committee agree with the views of the Department and feel that the Magistrates/Judges trying cyber cases need not be experts in that area as the basic exercise and technical intricacies of such cases are dealt with by the investigating officers and lawyers. However, they are of the opinion that the Department, in tandem with the industry, should take measures to initiate some basic training programmes for all those associated and dealing with cyber cases in order to enable them to understand and effectively handle the complexities of such cases.

(e) Spam

35. One of the important issues that has been brought to the notice of the Committee during the course of the examination of the Bill is that 'spam' or receiving unwanted and unwarranted e-mails has not been appropriately addressed in the proposed amendments. The Department's reply that sub-Section (b) of Section 66 A and Clause (i) of Section 43 of the Act appropriately address the issue pertaining to spam

does not convince the Committee as a close scrutiny of the above said two Sections reveals that the issue of spam has not been adequately dealt with. The Committee appreciate to note the Secretary, DIT's statement that it is very difficult to deal with spam as it can be generated from anywhere in the world. But in view of the irritation and agony that the recipients of unwarranted e-mails have to go through, the Committee are of the considered view that specific legislations should be incorporated in the proposed amendments to effectively deal with such mails. So far as generation of spam beyond the geographical boundary of India is concerned, the Committee feel that once the issue of jurisdiction of law, as has been broached upon elsewhere, is settled, that will automatically take care of this problem.

(f) Powers of Controller of Certifying Authorities (CCA)

36. While examining the Bill, the Committee received suggestions from some quarters that instead of vesting the powers of 'Controller of Certifying Authorities (CCA)' vaguely in the Central Government which has been otherwise so hard pressed, some concrete safeguards should be found out. The Committee also note that according to the Ministry of Law and Justice (Legislative Department), there is no need to vest the powers of the Controller of Certifying Authority in the Central Government. However, according to the Department of Information Technology, specific responsibility of licensing the Certifying Authorities for issue of digital signatures and regulating their functions has been assigned to the Controller of Certifying Authorities whereas the power to issue directions for interception or monitoring or decryption of any information through computer resources are being proposed to be

provided to the Central Government, interception being a larger issue. However, to avoid single point choking, the Central Government may provide the power to other agencies to deal with the cases in emergency situations. The Committee find that at present, the Department of Telecommunications, being the licensing authority for Internet Service Providers (ISPs), have been assigned with such powers of interception, monitoring, etc. The Committee are in agreement with the views of the Department that as the issues of monitoring, interception, encryption and decryption require input and coordination among different Ministries and Departments, the Central Government would be in a better position to coordinate that than the Controller of Certifying Authorities. However, the Committee feel that instead of using the words 'other agencies', it would be appropriate to identify three/four agencies alongwith the Department of Telecommunications, anticipating the technological evolutions and commensurate requirements so that there is no ambiguity in interpreting the law in this regard.

(g) Electronic Fund Transfer

37. During the course of the examination of the IT (Amendment) Bill, 2006, some industry representatives suggested to the Committee that there is a need for specific provisions in the law to legalise and enable electronic fund transfer and recognition of the concept of electronic payments, digital cash, electronic cash, electronic money or other existing systems of electronic payments. The Legislative Department are also of the view that there is a need for a separate Act for Electronic Fund Transfer (EFT) since certain transactional issues cannot be covered under the IT Act. The Department of Information Technology concur

with the views of the Legislative Department and are of the opinion that a separate Act for EFT needs to be drafted. In this context, the Committee are given to understand that the Payment and Settlement System Bill which will take care of the electronic fund transfer issues is going to be introduced in the Monsoon Session, 2007 of the Parliament for approval. The Committee hope that the proposed Payment and Settlement System Bill will adequately deal with the issues of electronic payments, digital cash, electronic money, and all other existing systems of electronic payments in order to address the concerns expressed by the industry. The Committee would like to be periodically apprised of the developments made in this regard.

38. To sum up, the foregoing paragraphs have identified several areas relating to the cyber law in general and the Information Technology (Amendment) Bill, 2006 in particular, which require necessary attention. These *inter alia* include, the need for a comprehensive, self enabling and people friendly IT law; urgent initiatives in materialising an International Convention against cyber crimes/cyber terrorism under the auspices of the United Nations; auditing of electronic records; data protection and retention; casting a definite obligation upon the intermediaries/ service providers; simplification of the Adjudication Process; making cyber offences cognisable under various Sections; retention of hacking in its original form; inclusion of 'child pornography' in the law and deterrent provisions against child abuse; and conferring powers of interception on the State Governments in tune with the provisions of Section 5 (2) of the Indian Telegraph Act, 1885; etc. The Committee trust that their observations/recommendations will be

examined in depth and necessary legislative proposals will be brought forth at the earliest with a view to ensuring an appropriate legal framework to address the cyber space.

New Delhi
31st August, 2007
09 Bhadrapada, 1929 (Saka)

NIKHIL KUMAR
CHAIRMAN
STANDING COMMITTEE ON
INFORMATION TECHNOLOGY