Proposed
Amendments to Information Technology Act-2000

You Be the Judge..
Is it Criminal Friendly? Or Industry Friendly?

Some see a Beautiful Girl in the above picture. Some see a witch in the picture instead ! Perhaps I taptly represents the Proposed Amendments to Information Technology Act which is being presented as a law will protect the Indian IT industry and provide confidence to the International public that India is safe for BPO business but in reality hides a criminal friendly legislation.

To Find out the truth, Read through this informative booklet.

Complied by Naavi, founder of www.naavi.org

Author:

Na.Vijayashankar (Naavi)

"Ujvala", 37, 20th Main, B.S.K.Stage I, Bangalore 560050

Founder, www.naavi.org, Chairman, Digital Society Foundation, Advisor, ITPF India

Disclaimer:

The contents of this book represent the views of the author based on the expert committee report for amendments to ITA-2000, presented in August 2005, which has passed through the Union Cabinet Committee and is expected to be placed before the parliament in the November 2006 session.

Any changes made to the recommendations of the committee by the Cabinet before being placed in the Parliament has not been taken into account.

I wholeheartedly welcome any changes that would render the comments made here in redundant.

Naavi
November 15, 2006

Contents

Chapter I

"I Love You" can Now Roam Freely in India

"I Love You" is the name of the famous virus which created havoc in the Internet world in 2000. The impact of the virus was so intense that a psychologist said that it has created a paronia in the Internet user's mind about e-mails. This virus was estimated to have created a damage of billions of dollars worldwide. It was the adverse publicity generated by this virus that prompted the Indian Government in May 2000 to rush through the passage of Information Technology Act 2000 in the parliament in a record two days without any worthwhile debate resulting in the passage of an act with several drafting errors.

Though the FBI was able to crack the case and trace the introducer of the "I Love You" virus to a student of an university in Phillipines, the perpetrator of the crime could not be punished since Phillipines did not have any law under which the person could be punished for the crime. Since then, Phillipines Government has introduced necessary laws to make "Virus Introduction" a punishable offence.

In the last six years after the "I Love You" virus made its appearance and India passed the Information Technology Act, the damage potential of viruses have only increased by leaps and bounds. Now Viruses spread faster so that before

their first identification and distribution of anti dotes, substantial damage is already caused. Secondly, Viruses have now become more sophisticated so that they can escape easy detection and cause more damage. Some are actually used as tools of stealing passwords and gaining entry to protected networks for committing Bank frauds and extortionist crimes.

In the light of these developments, if India was attempting a review of its six year old law, the expectation would be that the law against virus would be made stricter. But what is that the Government of India has set itself to do in the proposed amendments?. Let us see what the new law on virus in India looks like in the proposed amended section 66.

Proposed Section 66 (b) (i) states as under:

> *b) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is incharge of a computer resource*
>
> *(i) introduces or causes to be introduced any computer contaminant or computer virus into any computer resource;*
>
> *he shall be punishable with imprisonment upto two years or a fine which may extend up to five lacs or with both;*

Now compare this with the present section 66 which states as under.

"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking." And

"Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both"

If we forget the name of the crime under Section 66 (Present), the description of the offence covers any action of a Virus, Worm or Trojan since its effect on the system is to "Diminish the value" of information residing inside a computer or "Diminish the utility" of information residing inside a computer. Thus this section covered the offence of virus introduction with three year imprisonment as against the two years recommended now.

Apart from the reduction of the term of imprisonment, it must be noted that the present section 66 is applicable in all cases where the person introduced the virus intentionally or in the absence of intention, with a knowledge that "he is likely to cause wrongful damage".

As against this, the new section can be applied only when the virus has been introduced *"dishonestly or fraudulently, without permission of the owner or of any other person who is incharge of a computer resource"*.

In the case of the student who caused the "I Love You" virus, it is on record that the person stated when confronted by the Police that "I Love You Virus" was a part of the research project he was engaged in, that he had no intention of releasing the virus to the Internet and its movement from the lab network to the wild was an accident.

If this statement can be taken at face value it is clear that the accidental introduction of the virus into the wild cannot be an offence under the new provisions. On the other hand, under the existing provisions, since the person responsible for the introduction of the virus was a person with substantial software knowledge, it can be presumed by a Court that he had knowledge that "he is likely to cause" harm.

This case is similar to a person who is doing research on biological warfare and claims that a deadly strain of virus escaped to the atmosphere accidentally or a driver of a vehicle who causes death of pavement dwellers by rash and negligent driving but not with any intention of killing others.

Why the Expert Committee thought that "Negligent" or "Accidental" virus introduction should not be a punishable offence is a mystery.

The laws as at present would have placed a strict liability on IT users to use "Due Diligence" in protecting their computers and avoid spread of virus. This "Strict Liability" and the "Need for Due Diligence" is not required under the new provisions.

We can therefore conclude that "I Love You" virus can now roam freely in India and move from computer to computer with the person responsible claiming that it was an accident. There will of course be several eminent criminal lawyers who would come to the defense of such criminals and challenge the Court that "Unless the Crime is proved beyond reasonable doubt, the accused shall not be pronounced guilty.

The question of "Is it an accident? Or a fraudulent, dishonest and without permission conduct of the accused"? will always be confronting the future "Virus Offences" in India and tilt the judgments invariably in favour of the accused.

Happy hunting for Virus adventurists!.

Chapter II

"BPO Employees Selling data now have a good excuse"

Let us recall the two incidents in Gurugaon that have been instrumental to the amendments proposed for Information Technology Act 2000. The first was the sting operation by the SUN reporter from U.K. who accused one of the employees of a company called e-Infinity Search that he sold confidential data of some UK customers to him for a price. This incident evoked a global image backlash on Indian BPOs and their reliability to handle confidential data entrusted to them by the international data processors. The media hype on the incident was so much that the Prime Minister was forced to announce correction to our laws to prevent such happenings. This was also supported by many industry stalwarts. In the process of calling for the change of laws no body spared a thought to whether the existing laws really were incapable of meeting the requirements of punishing the accused if he was guilty or not.

In the aftermath of this incident and the Baazee.com incident in which the CEO of Baazee.com was arrested, the Government of India constituted the "Expert Committee" to review Information Technology Act 2000 and to suggest amendments ostensibly to provide assurance to the international community that India had suitable laws to meet the requirements of data protection.

Now in the aftermath of another sting operation again in Gurugaon, a company called Acme Tele Power Limited, one of whose employees was accused of "IP Theft" threatened to move out of India since it felt that their Information Assets are not getting necessary protection in India. Again, instead of analyzing what was the problem, Government announced that the "Expert Committee" report which was being held back because of the various deficiencies in the proposition since last one year would be passed in the coming session of the parliament. The required draft of the Bill was passed by the Cabinet Committee overnight.

Since the very purpose of the formation of the committee and its present push to the Bill status was dictated by the need to protect the security perception of Indian BPOs, it was presumed that the amendments would actually "Tighten Laws" and provide for "Data Protection".

But what is the reality? Does the proposed amendments tighten the laws? Or loosen it?. Let us see some of the provisions.

If an employee of a Company leaked confidential data and released it to unauthorized persons, it amounts to "Diminishing the Value of the information residing inside a computer" and hence comes within the purview of the present Section 66. Additionally, under Section 43, the person who has suffered financial damage on account of such a data leak can claim compensation upto Rs 1 crore.

It is therefore incorrect to say that there is no provision for punishment of such employees under the existing laws.

Now, let us see what the new provisions mean.

Firstly, punishment under Section 66 has been reduced from three years to two years. Secondly the preconditions such as "Dishonesty, Fraud and lack of permission" has been prescribed for applying section 66.

In the case of the e-Infinity Search, if one recalls the statement of the accused, he had stated that

> "He parted with a set of data which he considered as not 'live' and under the impression that he was presenting his credentials in a job interview to a prospective employer".

At face value therefore, he had not acted dishonestly or with fraudulent intentions. Hence if the new laws are implemented, the person cannot be arrested and booked under Section 66. This will now become a standard defense to any employee related data theft including the case where the data is passed on to a competitor. In fact, even in the case like the HSBC fraud in Bangalore where one Mr Nadim Kashmiri was arrested for altering some critical information in the Bank customer records which enabled some body else to fraudulently withdraw the money, the accused can take a defense that he was not aware that the changes were considered routine changes and not fraudulent manipulations.

The dilution of Section 66 therefore is a serious threat to safety of information asset owners.

There is also another proposed change which is hailed as "Data Protection Measure". This is the introduction of a new subsection 43 (2) which states as under.

> *" If any body corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, is found to have been negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore to the person so affected."*

Apart from the provision being applicable only to a "Body Corporate" and not an "individual" who runs a business where personal data is handled, it is attracted only when the body corporate is negligent in implementing and maintaining "Reasonable Security Practices". The Government is expected to spell out what is "Reasonable Security Practices" and What is "Sensitive Personal Information" before we can assess this section.

But since the existing provision already had a requirement that all IT users have to take reasonable precautions (Due Diligence under Sections 79 and 85) to prevent occurrence of Crimes and data leak was already a crime under Section 66, the newly added 43 (2) cannot be considered as some

thing new. At best we can recognize that instead of the concept of "Due Diligence" there is now the concept of "Reasonable Security Practices".

Further, While the concept of "Due Diligence" was a open, moving, industry driven bench mark, the reasonable security practice would be a static prescription by a committee of the Government which needs to be reviewed and upgraded from time to time. Failure to upgrade the guidelines would mean obsolescence of the security guidelines.

Thus 43 (2) is at best a clarification and does not add to the data protection aspects of the current version of Information Technology Act 2000.

Now we shall turn our attention at another new section introduced by the amendments namely Section 72 (2) which states as follows:

> *Save as otherwise provided under this Act, if any intermediary who by virtue of any subscriber availing his services has secured access to any material or other information relating to such subscriber, discloses such information or material to any other person, without the consent of such subscriber and with intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to the subscriber so affected*

Under the provisions of the above section, though the figure of RS 25 lakhs appear to be stringent, the liability arises only if the intermediary discloses information of the victim "with intent to cause injury to him" and not otherwise.

Thus if some girl has shared her photograph to a matrimonial site and the website owner allows the information to be wrongfully used because of lack of security at his end, then unless it is proved that he did it with an intention to cause injury to that girl, no offence is recognized. Same would be the case of a job site where the fact of a person having made an application for a new job may cause him injury.

Individual data owners may also have to confront the provisions of the new Section 79 which further dilutes the protection available to their sensitive personal data in the hands of body corporates who may claim as "intermediaries" since "Intermediaries" will not be liable under "any law" unless "conspiracy" and "abetment" is proved. (Discussed in greater detail in a separate chapter)

Thus, the claim that the new provisions would enhance data protection aspects of law is nothing but a myth. In reality the existing data protection aspects have actually been diluted and persons who cause data leaks have one or more excuses to escape the clutches of law.

Chapter III

"Hack, Crack and Enjoy !"

"Hacking" has always been considered a biggest threat to the Digital Society. In a way the term "Hacking" is almost considered a generic description of all Computer Crimes. After the notification of Information Technology Act 2000 with effect from October 17, 2000, in India, the word "Hacking" came to be associated as an offence under Section 66 of the Act.

While globally there was a distinction between "Cracking" which was malicious hacking, and "Hacking" which was a network security related activity to find out vulnerabilities, in India, "Hacking" had only one meaning and that was the offence under section 66 of Information Technology Act which stated as under.

> *"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking." And*
>
> *"Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both"*

The new version of the Section 66 as proposed by the amendments is as follows:

66 Computer related offenses:

a) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is in charge of a computer resource

(i) accesses or secures access to such computer resource;
(ii) downloads, copies or extracts any data, computer data base or information from such computer resource including information or data held or stored in any removable storage medium;
(iii) denies or causes the denial of access to any person authorised to access any computer resource;

he shall be punishable with imprisonment upto one year or a fine which may extend up to two lacs or with both;

(b) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is in charge of a computer resource

i)introduces or causes to be introduced any computer contaminant or computer virus into any computer resource;

ii) disrupts or causes disruption or impairment of electronic resource;

iii) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer resource;

iv) provides any assistance to any person to facilitate access to a computer resource in contravention of the provisions of this Act, rules or regulations made thereunder;

v)damages or causes to be damaged any computer resource, date, computer databse, or other programmes residing in such computer resource;

he shall be punishable with imprisonment upto two years or a fine which may extend up to five lacs or with both;

If we compare the two versions of Section 66 it is clear that the existing section applied to any type of offence in which information residing inside a computer was adversely affected by any means. It also applied when there was no intention but "Knowledge" that a wrongful harm was a likely result of an action. The section was therefore very broad and attracted any type of offence even some which were not even known in 2000 when the act was drafted.

The new version on the other hand tries to bifurcate offences into two categories one carrying one year

imprisonment and the other carrying two years imprisonment as against the current three years. Also instead of the description of the offence in general terms such as “Diminishing the value or utility”, “Affecting Injuriously” etc, the new section tries to specifically describe eight types of offences. These segmentation of offences to eight types cannot add anything to the current description in terms of coverage of unknown offences. It can leave room for some loopholes which can be exploited by criminals. It would also be very ineffective when it comes to tackling community crimes such as Cyber Terrorism, mass defacement, virus attacks, denial of service attacks etc where individual motive against the affected party is either non existent or difficult to be proved.

The most important aspect of change is the removal of the operation of “Negligence” as a possible cause of criminal action leaving scope for criminals to hide behind technicalities of “Accidents”, “Vulnerabilities”, “Software Bugs” etc.

The introduction of the words “Without Permission” leaves scope for authorized activities which may turn sour. Thus an “Ethical Hacker” may commit a mistake causing damage and escaping liability for his negligence.

Hackers will henceforth have a soft law in India to contend with.

Chapter IV

"Be an Intermediary and Be Immune to Liability"

One of the most important aspect of the proposed amendment is the zealousness with which it tries to protect Intermediaries of all kinds from offences of all kinds.

For example the new Section 79 states as follows:

79. Exemption from liability of intermediary in certain cases

1. *An "Intermediary" shall not be liable under any law for the time being in force, for any third party information, data, or link made available by him, except when the intermediary has conspired or abetted in the commission of the unlawful act.*

2. *The provisions of sub-section (1) shall apply in circumstances including but not limited to where:*

   a. Intermediary's function is limited to giving access to a communication network over which information made available by third parties is transmitted or temporarily stored; or The intermediary:

(i) does not initiate the transmission,

(ii) does not select the receiver of the transmission, and

(iii) does not select or modify the information contained in the transmission.

3. The provisions of sub-section (1) shall not apply if, upon receiving actual knowledge of, or being notified by the Central Government or its agency that any information, data or link residing on a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails expeditiously to remove or disable access to that material on that resource.

***Explanation**: For the purpose of this section:-*

a. Term 'Intermediary' has been defined in Chapter I, Section 2(w).

b.'Intermediary' shall include, but not limited to, telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines including on-line auction sites, online-market places, and Cyber Cafes.

c. 'Third Party Information' means any information dealt with by an intermediary in his capacity as an intermediary.

Note the words “Under any law” in the first sentence of the section. It appears that the Intermediaries are being provided immunity from any law in force unless conspiracy and abetment is proved. This could mean that even in cases of drug peddling and terrorism, it is doubtful if the intermediary can be held liable.

The definition of "Intermediary" is wide enough and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines including on-line auction sites, online-market places, and Cyber Cafes.

The list does not extend to IT Companies though they may be operating under a network unless they re-define their work as that of an "Intermediary". The provisions of immunity from offences will therefore not be available for traditional IT companies but only to Intermediaries such as Portals.

At a time when terrorists are freely using Cyber Cafes for their nefarious activities, while the existing laws made them liable to observe “Due Diligence”, the proposed laws try to discharge them from even the responsibility of “Due Diligence”.

If the proposal is passed, then the Cyber Café regulations passed by some states may become redundant and has to be withdrawn.

Terrorists and Naxalites may be immensely pleased with these provisions so that they can operate from friendly cyber cafes enjoying all immunities that one can expect to prevent any Policeman trying to get tough.

Chapter V

"Let Police Go to Hell"

Police in any system are an important component of a law abiding society. While law is essential for any society, it needs to be enforced by the Police and Judicial systems. Unless both these wings are strong enough laws have no meaning since they remain on paper.

At the same time, there are instances where Police are known to abuse law as much as any other segment of the society. If this tendency develops because the law is too stringent, then one must look for ways and means of reducing the abuse of law. Obviously the solution for abuse of law by police is not eliminating the police but making them more responsible.

But what does the new Information Technology Act propose in respect of powers of Police?..

In the present version of Information Technology Act 2000, section 80 specified the powers of the Police to search and arrest without warrant for offences under the Act. It restricted the powers only to a "Public Place" and to be exercised by Officers not below the rank of "Deputy Superintendent of Police". The provisions therefore were very reasonable.

In the new provisions the section 80 is sought to be deleted without any corresponding provision stating the powers of Police. Additionally, under Section 72 it is stated that a victim needs to complain to a Magistrate instead of a Police Station.

Further, the period of imprisonment under most sections of the Act have been reduced to indicate that Cyber Crimes are now considered less menacing than before. Accordingly, imprisonment under Section 66 is reduced from three years to one and two years and under Section 67 from five to two years. These changes have been made so that Police cannot apply the "Three Year Rule" to consider an offence as "Cognizable" and arrest any persons.

These changes collectively indicate that the changes have been made to curtail the powers of the Police so that Police are not empowered to conduct search, seizure or arrest without warrant under any provisions of the Act.

However, under the absence of a specific mention of the reason for the deletion, there is a confusion whether this deletion can be interpreted as to mean that the powers of arrest etc will now be available as per the Criminal Procedure Code with the station house officer. Since the imprisonment period is anyway less than three years in most cases, it does mean that the powers of arrest without warrant cannot be applied except in a few cases such as Child Pornography.

But the current section 78 remains stating that investigation of offences under the Act are restricted to Deputy Superintendents of Police only. So it is difficult to interpret that an Inspector in charge of a Police Station can effect an arrest while he has no powers of investigation.

The extent to which Police are treated as dirt can be seen from the seemingly innocuous change sought to be made in Section 69 which deals with providing assistance of the Controller in certain cases for the law enforcement. The new provisions deliberately remove the words "for preventing incitement to the commission of any cognizable offence" from the list of occasions where the assistance of the Controller can be sought. If therefore the Police need the assistance of the Controller in case of any Crime, Controller is not bound to provide the same.

It is therefore to be interpreted that the proposed amendments have been made with the objective of taking away all powers of arrest and search from any rank of the Police while the investigations are still to be undertaken by officers of the rank of Deputy Superintendents of Police.

The net impression that the proposed changes communicate is that we do not need active and powerful Police to take charge of Cyber Crime management.

Probably this will be one single reason that many other companies like the Acme Tele Power of Gurugaon would like to shift out of the country and if it happens, the responsibility would squarely on the "Expert Committee"

for putting up suggestions that weaken the Law and Order situation in Indian Cyber Space and the Government for its unimaginative way of accepting such recommendations.

Chapter VI

"Abuse of Women?.. Law will take its own course"

From the history of Cyber Crimes in India, it is observed that women have been the center of web based attacks leading to defamation, ragging and harassment.

In the initial days Police took action under Section 67 of Information Technology Act 2000 to book any website owner or cyber café or an individual using the Internet for promoting obscenity. A conviction under Section 67 was also achieved by a Chennai Court where a boy had posted a message on yahoo e-group causing annoying phone calls to a girl. Recently the SMS related harassment was also being sought to be curbed under Section 67 bringing some relief to women in India.

Knowing the ease with which a person can send hundreds of e-mails about a girl often with morphed pictures and the sensitivity of the society to such scandals, there was a need to curb this tendency with an iron hand.

Unfortunately, the proposed amendments appear to move in exactly the reverse direction where there is reduction of sentence for obscenity related crimes, exemptions for certain categories of persons from liability and placement of hurdles in the path of women who would like to fight for

justice as if protecting the honour of women is not a priority.

Let us see how amendments lead us to such a conclusion.

Firstly section 67 which deals with "Obscenity" has been amended. A new subsection (2) has been added to include "Child Pornography" as a separate offence. In the sub section (1) the words "Save as provided under Section 79" has been added.

The new provisions read as under:

Publishing in electronic form of information which is obscene

> *(1) Save as provided in this Act under Section 79 which exempts intermediaries from liability in certain cases, whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five*

years and also with fine which may extend to ten lakh rupees.

(2)Whoever intentionally and knowingly publishes or transmits through electronic form any material which relates to child pornography, shall be punished with imprisonment for a term not less than three years and with a fine which may extend to ten lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

The new provisions under 67 (1) make this section subordinate to section 79 so that "Intermediaries" cannot be held liable except when there is conspiracy and abetment. Additionally the period of imprisonment is brought down from five years to two years in first instance and from 10 years to 5 years in the second instance of the crime.

The protection available for misuse of electronic documents to propagate obscenity is therefore grossly diluted.

Additionally under section 72 the new provisions define certain actions bordering on obscenity is defined as "Breach of Privacy" and certain punishments are prescribed. According to Section 72 (3),

> *Whoever intentionally captures or broadcasts an image of a private area of an individual without his consent, and knowingly does so under circumstances violating the privacy of that individual, shall be liable to pay compensation not exceeding Rs. 25 lakhs to the person so affected, and shall also be liable for imprisonment for a term not exceeding one year or with fine not exceeding Rs 2 Lakhs, or with both on the complaint of the person so affected.*

The effectiveness of this section is however blunted by section 72 (4) which states

> *No court shall take cognizance of any offense punishable under sub-section (3) except upon a complaint filed by the aggrieved person in writing before a Magistrate*

Thus on the one hand, "Capturing" of an image of a private area of an individual is made punishable but the remedy bypasses the Police and requires a direct approach to the Court. Secondly it is important to note that "Capturing" is not restricted to "Electronic Capturing" and hence any kind of photography could be brought under this provision. The section goes on to define "private area" of a person leaving enough scope for "obscenity" without technically violating the section.

In contrast, Section 67 with its relative definition of what is obscene is more than adequate to protect the interests of women from being exploited through electronic exposures.

Perhaps the law makers thought that there is no need for such protection as the law will take its course and protect them from exploitation.

Chapter VII

"If I have money, no jail can keep me in for a Cyber Crime"

In Criminal justice system there is a provision for "Compounding of Offences" where by the accused may enter into a compromise with the prosecutor and pay an additional sum of money in return of remission of the prison sentence. Normally this is preceded with the compromise between the victim and the accused.

The principle of compounding is meant for non grave offences where the accused might have undergone a reformation process before the finalization of the trial and the victim also feels that imprisonment is not warranted.

However, in the proposed amendments there is an uncomfortable feeling that the principle of Compounding is being used to let criminals with money escape imprisonment.

In the present version of the Act, compounding is permitted for civil liabilities coming under Chapter IX of the Act. There is no compounding for the criminal offences under the Chapter XI of the Act.

However it is now proposed that compounding be permitted for both the Civil and Criminal offences and the compounding authority is the "Adjudicator" or the "Controller". Further "Compounding" can be done without

the need for consent from either the complainant or the victim or even the court if the subject dispute is already under trial.

It is provided under Section 80 A of the proposed amended act as under:

80A. Compounding of Certain Offenses

(1) Notwithstanding any thing contained in the Code of Criminal Procedures, 1973, any offense punishable under this Act may either before or after the institution of any prosecution be compounded by

(a) the Controller; or

(b) the adjudicating officers appointed under section 46, where the maximum amount of fine and/or imprisonment does not exceed such limits as may be specified by the Central Government.

on payment or credit to the Central Government of such sum as the Controller or the Adjudicating officer, as the case may be, may specify.

(2) Nothing in sub-section (1) shall apply to an offence committed by a person within a period of three years from the date on which a similar offence

committed by him was compounded under this section.

Explanation: For the purpose of this section

any second or subsequent offence committed after the expiry of a period of three years from the date on which the offence was previously compounded, shall be deemed to be a first offence.

(3) Where any offence is compounded before the institution of any prosecution, no prosecution shall be instituted in relation to such offence, either by the Controller or by the adjudication officer or by any other person, against the offender in relation to whom the offence is so compounded.

(4) Where the composition of any offence is made after the institution of any prosecution, such composition shall be brought by the Controller or the adjudicating officer in writing, to the notice to the Court in which the prosecution is pending and on such notice of the composition of the offence being given, the person in relation to whom the offence is so compounded shall be discharged.

Already the civil contraventions under the Act was outside the purview of the Courts until the appeal stage where the High Court would come in. Now with the Criminal offences also going out of the judicial supervision at the

trial stage, the entire Cyber Crime justice system will be in the hands of the adjudicators.

At present the adjudicators are the IT Secretaries of different state Governments who are working under their respective political bosses. This provides scope for influence of various kinds acting on an honest officer. Hence there is a possibility that the Compounding provision could vitiate the process of justice in Cyber Crimes.

It is also a practical observation that Adjudicators have little time for the Cyber Crime trials amidst their present commitments. Some disputes are between a member of the public and the state where there is a conflict of interest. Some times the dispute may be with a company from which state expects certain investments which the IT Secretaries themselves negotiate in the course of their natural duties. It is therefore difficult for the IT Secretaries to manage the Cyber Crime justice system without conflict.

For all these reasons, out of all the provisions of the proposed amendments, one that makes us gasp in disbelief is this blatant attempt to take over the Cyber Crime justice system from the judicial to the executive level without proper checks and balances.

In the long run this will lead to arrogant wealthy criminals taking law into their hands and walking away with a compounding deal with the executive with their money and

political power. The future of Cyber Crime Justice in India therefore appears to be dark.

Chapter VIII

"Your character is known by the friends you reject"

Having expressed the reservations about the proposed amendments in strong terms, it is necessary to answer the doubts if Government was forced to take up the amendments as proposed by the "Expert Committee" because this was the best advise they could garner from the market. Also it is necessary for the uninitiated to understand if there were any larger issues that the Committee or the Government ignored in preference to what was finally chosen since this can give us some idea of why the Government could have thought of a legislation which could be criticized as "Criminal Friendly".

The following set of suggestions which were placed before the Ministry of Communications and Information Technology during the period the "Expert Committee" was in session indicate the suggestions that the Committee ignored in preference to what they finally recommended.

1. **Recommended for Spam Regulation:**

"Spamming" is related to "Marketing", "Freedom of Speech" and "Privacy Rights". It is necessary to therefore bring legislation on controlling "Spam" without affecting the genuine right to use the Internet media for marketing both for commercial, social and political purpose.

Similarly, the legislation should not curb the freedom of speech while upholding privacy of individuals.

The suggestion on "Spam Control" therefore includes modalities for managing genuine use of Internet as a communication medium through a "Bulk E-Mail Licensing Programme".

It is open for the Government to designate the CCA (Controller of Certifying Authorities" as the appropriate authority for the purpose of Spam Control.

XY) Sending Unsolicited Electronic Messages:

Except under a valid **Bulk E-mail license** from an **appropriate authority**

Whoever,

1) Sends or causes to send an **unsolicited** electronic message/s of any description with a source **identity that is not disclosed**, or

2) sends or causes to send an unsolicited electronic message/s of any description after the addressee has **duly notified him of his intention not to receive such communication** as prescribed under this Act, or

3) Except under **an express consent** of the recipient, sends or causes to send an electronic message/s of any description containing information that is **obscene or offensive, that may defraud or is intended to defraud, that may cause or is intended to cause distress, that may break or is intended to break any law in force or that may otherwise create disharmony in or harm to the society or cause harm to the integrity of the nation and friendly relations with other countries,**

shall be punishable under this Act with any or all of the following

a) Payment of compensation or damage to each of the person/s affected by the offence subject to a maximum of Rs 1 lakh per person.

b) Imprisonment subject to a maximum of Two Years

c) Fine subject to a maximum of Rs 2 lakhs

Notwithstanding the punishment or penalties mentioned above, if the offence as defined under (XY) above results in or is intended to result in an act that is an offence under any other law in force, the offender **shall**

also be liable for punishment or penalty to which the offender is liable under such laws.

Provided however that if any message is caused to be transmitted by mistake of fact or due to technological factors beyond the reasonable control of the person in whose name the message is sent, no offence would be recognized if such a person proves that the message was sent **without his knowledge and he had exercised all due diligence** to prevent commission of the offence.

Explanation:

For the purpose of the section (XY) above,

a. the disclosure of source identity is considered sufficient if a reply can be sent to the disclosed source address and such reply does not bounce.

b. an addressee may communicate his intention "not to receive" a communication through a digitally signed message or in any other manner that may be laid down for the purpose and unless specified, such notice shall expire after 3 months.

c. the unsolicited message shall be admissible as evidence in a Court of law even if it is not digitally signed. *(Ed: corresponding change required to be made in Indian Evidence Act)*

d. the intermediary who causes the unsolicited messages to be transmitted shall also be liable under the Act as if the offence was committed by them unless he proves that the offence was committed without his knowledge and the intermediary had exercised all due diligence to prevent commission of the offence.

e. a message is considered "solicited" if it may be inferred from the conduct and existing business or other relationship of the recipient that he consented to such messages being sent to him.

f. "Express Consent" in sub clause (3) means only a consent obtained through a manually entered affirmative expression.

g. "Appropriate Authority" for the purpose of this section shall be the "Controller of Certifying Authorities" or any other authority specifically designated for the purpose by an order of the Government of India.

2. Suggested for Prevention of Cyber Squatting:

"Cyber Squatting" is related to "Trade Mark Rights". Further, any law passed on "Cyber Squatting" in India will interfere with the "Uniform Dispute Resolution Policy" which is a contractual obligation to which all domain name

registrants are presently subjected to. It will also affect the rights of Indians who have to face charges of "Squatting" in respect of international generic domain names such as dot com, dot org etc.

Any law attempted here should therefore be such as not to unduly create a harassment of Indian Citizens.

It is suggested that a Section may be introduced in Chapter IX to the following effect:

(PQ)Whoever, in bad faith and with the intention

to cause disrepute, harm to another person or

cause disruption of any legitimate business or

cause confusion in the minds of the public, who having regard to the circumstances, are likely to be influenced

registers a domain name

shall be liable to pay damages to the person so affected not exceeding Rs 10 lakhs

and for the purpose of this section, a person not being a resident of or a citizen of India shall also be liable even if no computer or computer system located in India is used for the contravention.

Explanation:

For the purpose of this section exercising of due diligence including appropriate disclosures shall be considered as indications of lack of bad faith.

3. Cyber Terrorism:

There is a need for defining the offence of "Cyber Terrorism" and punishments therefore.

Suggestions in this regard are as follows:

A Section to be introduced in Chapter XI to the following effect:

(MN) Whoever

> uses a Computer or any associated device or an Electronic Document to create destabilization of the economy or any segment there of, intimidate or coerce a government, the civilian population, or any segment thereof, or to create disharmony in the society, in furtherance of political, religious or social objectives or to harm the community injuriously by any means shall be liable for imprisonment upto 10 years or and fine upto Rs 100 lakhs

4. Data Protection:

It is recommended that a separate "Data Protection Act" may be considered with a definition of "Privacy Rights "of Indian Citizens defining responsibilities of data intermediaries, processors and users.

Information Technology Act recognizes "Data Theft" as an Offence under Section 66 and as a Contravention under Section 43. Digital Signature provides the means for data encryption and accountability in storage and transmission. Adjudication covers the need for quick dispensation of justice in respect of civil liabilities. Hence there is adequate coverage of data theft from the point of view of the industry.

Hence no amendment is required in the Information Technology Act on this account.

However, if it is considered expedient to pass an amendment to assure the International community that India has strengthened the laws after the recent incidents, an amendment may be suggested to provide some clarification on data protection as an expansion of Section 43.

Suggested that the following section may be added in Chapter IX:

(XY)

Whoever, collects, stores, processes or otherwise manages data of personal nature belonging to a data subject, in any manner shall take such steps as may be necessary to ensure that the data is collected on a strict need basis, stored securely and accessed only on a need to know basis and in the event such data is compromised, shall be liable to pay damages to the data subject for a sum not exceeding RS 1 crore.

5. Cyber Stalking

In order to cover the offence of "Cyber Stalking", an explanation may be added to Section 66 as follows.

"The term "Affecting injuriously" in this section includes use of any electronic information in a manner that causes harm, discomfort, harassment, threat or coercion to any other person".

6. Abuse of Power by Police

Section 80 of the Act provides powers to certain enforcement officers including non Police officers of State or Central Government to arrest any person and search and seize any property in public place on the grounds that in his opinion, an offence has been committed or is being committed or is about to be committed. Provision to prevent abuse of this provision is required and therefore the following suggestion is being made.

After Section 80, a sub section (4) may be added as to the effect that "Any officer who takes action under this section to arrest or seize property without sufficient justification shall be punishable with an imprisonment of 6 months or a fine of RS 1 lakh or both"

7. Interception of Communication

The powers for interception given under Section 69 of the act may be expanded to include

a) Pornographic sites
b) Fraudulent sites
c) Any other site that abets commission of any offence in India

Though this is implied in the section, an amendment to the following effect is recommended.

"The word "Cognizable Offence" in 69 (1) is recommended to be replaced with "Offence under any law in India"

And an explanation may be added to state that

"The term "Interception" under this section shall include "Blocking" of a site at any of the intermediaries or mandating of "Display of statutory notices" with the content displayed either through the intermediaries or otherwise"

The powers under this section can be exercised by a "Competent Authority" which shall be the Secretary of Information Technology or Home Affairs.

In order to prevent abuse the powers of "Interception of Communication" under section 69 of the Act, it is proposed that

a) A police officer not below the rank of Superintendent of Police supervising the investigation of any offence under this Act may submit an application in writing to the Competent Authority with necessary particulars for an order authorizing or approving the interception of wire, electronic or oral communication by the investigating officer when he believes that such interception may provide, or has provided evidence of any offence involving a terrorist act.

b) The permission when granted shall be for a limited time period not exceeding 60 days at a time.

c) The Competent authority may reject the application of the Police officer if he does not find sufficient grounds to approve the request.

d) The competent authority himself has to submit a copy of the order to a review committee within 7 days for approval.

8. Cyber Regulations Advisory Committee: (CRAC)

It is recommended that CRAC shall meet at frequent intervals not later than once in a quarter and review the working of the regulations and submit a report to the appropriate authorities. CRAC may also be designated as the "Review Committee" to review the orders on the interception of communication under Section 69 of the Act.

9. Secured Digital Signature:

Consequent to the notification regarding "Secured Digital Signature", the evidentiary value of an ordinary digital signature as per Section 85 B has been removed.

Accordingly, it is recommended that Section 85 B of the Indian Evidence Act may be amended to replace the words "Secure Electronic Record" with "An electronic record secured by a Digital Signature" in Para (1) and 2(b) and the words "Secure Digital signature" with "Digital Signature" in Para 2(a) and 2(b).

10. Cyber Marriage

There has been an intense debate recently on the feasibility of marriages and divorces happening on the Internet.

Existing laws make it possible to have Contractual marriages wherever allowed (Muslim marriages) to be concluded through digitally signed electronic documents.

Registered marriages are also possible through a similar digital marriage registration office.

Already divorces in Muslim community through e-talaqs have been approved by certain courts.

Considering the social implications, it is suggested that Cyber Marriages and Cyber Divorces should be notified as "Exempted from the provisions of ITA-2000 under Section 1(4)".

11. Civil Liabilities:

In order to make all criminal offences under the Act also liable for civil liabilities, the following amendment can be made to add section 43(A) under Chapter IX:

"Whoever commits any offence under any of the sections under Chapter XI of this Act shall also be liable to pay damages to the extent of RS 1 crore to the person so affected."

In order to provide for compensation in excess of RS 1 crore where required, an amendment may be added as Section 45 A

"Where the actual damage suffered by a person under any contravention of the Act is more than Rs 1 Crore, such claim of damages in excess of Rs 1 crore shall be a subject matter of an appeal on the adjudicator's decision"

It is noted that in its wisdom, the Expert Committee considered that issues such as raised in the above suggestions were of no relevance at this point of time for amendments to Information Technology Act and the Government of India agrees with it.

The depth of the thoughts that have gone into the formation of the recommendations of the amendments in its present form need to therefore be looked in this perspective.

Chapter IX

"Is there a silver lining to the dark cloud"?

Having explained the innumerable aspects of the proposed amendments which are detrimental to the interests of the public, it is necessary to also comment briefly if there are any benefits at all that are envisaged under the proposed amendments.

It is very difficult however to find some positive features that are worth mentioning. However some analysts consider that defining "Electronic Signatures" as a means of authentication and "Digital Signatures" as one of the permitted systems of "Electronic Signatures" as a positive feature.

Since at the present point of time there is no alternative for Digital Signatures (Hash and Asymmetric Cryptosystem based authentication), there is no immediate benefit envisaged under the proposed change. However, the change gives room for some fresh thinking on the subject and hopefully some innovative alternatives to the present system may be born. This can therefore be considered as a welcome step.

Second positive aspect which has caught the analysts attention is the introduction of the "Digital Evidence Examiner" concept to provide testimony in the case of Electronic evidence. Though not considered critical, if the terms for appointment of Digital Evidence Examiners is

properly drafted, it can be a beneficial addition to the present provision.

Perhaps these two provisions can be considered as the silver lining in the otherwise dark cloud.

Chapter X

"We need a Butcher's knife to protect Cyber Crime Law in India"

Now that we have dissected the proposed amendments and its criminal friendliness along with the neglect of the pressing issues and an attempt to take over Criminal justice management from the judiciary to the executive, is laid bear before you, it is time to think of what is the remedy at this point of time.

Now that the Union Cabinet committee has already taken a stand on the proposals and decided to place it before the Parliament, unless the Cabinet Committee reverses its decision, the matter will come before the members of the Parliament. When Information Technology Act was passed in May 2000, there was hardly two days given to the members to pass the legislation and before any body could understand what was in it, the ruling party had pushed it through the two houses.

If this time also the present Government considers it as a prestige issue, it may get the amendments passed without any fruitful debate.

The first thing that is required to be done therefore is for the Parliament to refer the Bill to a select committee of

parliamentarians who can get public views on the subject and then re present the Bill with modifications.

However, since the changes to be made are many, it is considered desirable if the entire set of amendments are scrapped and a fresh exercise is initiated for drafting the amendments ensuring a better team of experts to go through the provisions.

It is recommended that this should be a committee formed under the CRAC since the Act considers CRAC as the body which is to be referred for all such major amendments.

It is therefore recommended that we wield the butcher's knife and kill the present draft in to to and start a fresh exercise.

About the Author
NAAVI

Naavi is an E-Business Consultant based presently in Chennai, India. An Ex-Banker and a Financial Services Expert, Naavi worked as a Merchant Banker and a Financial Products Marketing Consultant for a better part of his long corporate career.

Naavi is the founder of Cyber Law Portal www.naavi.org, Cyber Law Education center www.cyberlawcollege.com and several service concepts such as www.lookalikes.in and www.ceac.in

He is the author of the first book on the subject of Cyber Laws in India and several other books subsequently.

He is a regular guest faculty in a number of educational institutions and conducts Cyber Law Courses in association with several law colleges in Karnataka

Naavi assists Police when required in Cyber Evidence Collection and interpretation to judicial standards. He also offers services to Companies for conducting Cyber Law/Security programmes and Compliancy Consultancy.

Naavi is also the founder secretary of Cyber Society of India, Founder Trustee of IIIT Law and Founder Chairman, Digital Society Foundation.

Naavi can be contacted at naavi@vsnl.com.