# SYNOPSIS ON EXISTING LACUNAE IN THE INFORMATION TECHNOLOGY ACT,2000 & REGULATIONS FRAMED THEREUNDER & CYBERLAW ENFORCEMENT IN INDIA-

# AUTHOR'S RECOMMENDATIONS TO STRENGTHEN CYBERLAWS IN INDIA


By **Karnika Seth, Cyberlaw expert & Advocate, Supreme Court of India**

Visiting Faculty, NIA, CBI, National Police Academy and National Judicial Academy

Author of *'**Computers, Internet & New Technology Laws'***, 2012 , Lexis Nexis

*Contact details*-

*Office address*- Seth Associates, Advocates & legal consultants

B-10 Sector 40, NOIDA-201301

*Mobile*: 9810155766 *Office*: 01204352846 *e-mail*: karnika@sethassociates.com


**SYNOPSIS ON EXISTING LACUNAE IN THE INFORMATION TECHNOLOGY ACT,2000 & REGULATIONS FRAMED THEREUNDER & CYBERLAW ENFORCEMENT**

# IN INDIA- AUTHOR'S RECOMMENDATIONS TO STRENGTHEN CYBERLAWS IN INDIA

By**Karnika Seth, cyberlaw expert & Advocate, Supreme Court of India**

## Introduction

India's Information Technology Act( IT Act,2000)isbased on the UNCITRAL Model Law of e-commerce whichprovides legal recognition to electronic documents and e-contracts. It provides legal framework for governing electronic transactions over Internet and for appointment of different functionaries under the Act to carry out their set of statutory duties. The Act also provides various Sections dealing with contraventions and offences such as computer related offences, punishment for publishing obscene content to punish offenders.Important amendments were made in the year 2008 in the said Act , such as introduction of new Sections pertaining to offences such as Child pornography[1], Cyber Terrorism[2], Identity theft and power to investigate was vested with Inspector and above rank.

Despite the fact that IT Act,2000 has been in existence since 14 years, the cybercrimes have been on the rise and law enforcement continues to face many challenges due to existing lacunae in the Act, absence of required rules which the Government needs to frame and unreasonable delays in appointment of key functionaries such as the non functionalCyber Appellate Tribunal since 4 years. India needs to adopt proactive steps to make Cyberlaw enforcement more efficacious. Given hereinbelow are Author's key recommendations that may be adopted to strengthen IT laws in India.

## 1. India needs to sign a Cyber Crime Convention

Many cybercrimes are committed cross border by persons located in other countries but India lacks cooperation in cybercrime matters from other countries as it has not signed any Cybercrime Convention till date.As a result, investigation and prosecution of cybercrimes (under IT Act,2000) committed by persons abroad becomes practically impossible. India is signatory to the United Nations Convention againstTransnational Organized Crime that addresses terrorism, drug trafficking and other serious crimes but does not deal specifically with cybercrimes.The provisions of the United Nations Convention againstTransnational

[1] Section 67B of IT Act,2000
[2] Section 66E of IT Act,2000

Organized Crime are inadequate for tackling cybercrime matters which requires prompt action failing which electronic evidence can be easily tampered/destroyed or become unavailable due to overwriting of logs by Internet service providers. A Cyber crime Convention or Treaty is imperative for making effective the Investigation and prosecution of cross border cybercrime cases. The global service providers such as Google and yahoo ought to assist in law enforcement processes and provide information required for cybercrime investigations. On several occasions, service providers claim that their servers are based abroad and they are unable to provide data till subpoena orders are taken from the courts within their jurisdiction.Signing the Cyber Crime Convention will expedite processing of cooperation requests made by India from other jurisdictions.Our existing MLAT process ( Mutual Legal AssistanceTreaty process) is too slow for tackling cybercrime cases.

## 2. Strengthening National Security and Incident Response

Computer Emergency Response Team and National Nodal centers need integration with Foreign Nodal centers and thrust should be on building a strong international incident response team that works with INTERPOL. Active surveillance of online forums,chat rooms should be made by the law enforcement to prevent misuse of social media. Social Media is being abused by recruiting of terrorists as evident from reported *Kalyanrecruitees* case and mandatory obligation to conduct due diligence to detect cyber terrorist activity must be placed on all Internet Service providers, including those that allow posting of third party content.

Establishment of a global Critical infrastructure protection mechanism will be instrumental in combating cyberwarfare and cyberterrorist attacks. Initiatives such as the Crime and Criminal Tracking and Network Systems(CCTNS) originally built for improving functioning of police stations will play a vital role in strengthening enforcement of cyberlaws in India.Its efficiency can be better if *CCTNS is expanded to include* limited access to banks and Internet access providers , cyber café and other stakeholders so that no services may be provided to cybercriminals and phishers ( who steal money by duping people online) whose records can be found on conducting due diligence through CCTNS.The Crime and Criminal Network And Tracking System, and the proposed NAT Grid systems will facilitate better coordination

between law enforcement agencies including police stations, leading to coordinated investigation. It currently aims to integrate coordination between police stations, immigration authorities, courts, telecom, hospitals, transport authorities, and citizens[3].

Another positive step is the creation of network whereby Delhi police can directly intercept internet communications instead of requesting information from Internet Service Providers (ISPs)[4]. However, abuse or misuse of the network needs to be checked and if interceptions are conducted strictly in the manner prescribed it will make legal enforcement and investigations of cybercrimes more effective. Such a systemcan be introduced and streamlined on a national level in the near future.

As on date,unification of cyberlaw through multilateral treaties and conventions is required to effectively combattransborder cybercrimes, including hacking, money laundering and phishing scams. Although Online Dispute Resolution may not resolve criminal cases , it can be still be used to resolve civil claims for compensation or recovery (particularly where disputes involve small claims) through virtual institutions such as such *cybersettle*[5]*etc*.

## 3. Electronic signatures yet to be notified

Pursuant to Amendments made in the IT Act in 2008,the Central Government of India is yet to notify other valid and recognized modes of electronic signatures other than digital signatures based on PKI infrastructure[6] and to define security procedures under Section 16 of IT Act, 2000 that will be used to create 'secure electronic signatures' which bear a favourable presumption in law of its authenticity under evidence law.As on date, no notification has been passed by the Central Government notifying other valid means of authentication of electronic documents apart from digital signatures although amendments took place way back in 2009.

---

[3] National Crime Records Bureau, Ministry of Home Affairs, "Crime and Criminal Network And Tracking System ",http://ncrb.nic.in/cctns.htm ( accessed on 1 Dec2014.)

[4]Neeraj Chauhan, "Delhi Police plan email intercept system",Times of India, Nov 11, 2011, http://articles.timesofindia.indiatimes.com/2011-11-11/delhi/30386285_1_intercept-delhi-police-internet-communications( accessed on 1st Dec 2014)

[5]www.cyber**settle**.com

[6] See Second Schedule of the IT Act,2000 as amended by IT (Amendment ) Act, 2008 wef 27-10-2009

## 4. Too short/not notified data retention periods

The IT (Intermediaries Guidelines) Rules,2011require an Intermediary to preserve the information it transmits on receipt of a complaint for *90 days* for investigation. However, in my view the period of retention too short to conduct anycyber crime investigation. Further,the rules donot provide for *any data retention period* for maintenance of logs in the ordinary course of business by internet service providers under Section 67©of IT Act,2000 which is imperative for effective cyber crime investigation & prosecution. The Central Government has not framed any rule for minimum data retention period by service providers such as Airtel, etc under Section 67© Of the IT Act,2000. As a consequence,in many cases, electronic evidence cannot be gathered as the data is overwritten by Internet service providers as per their own self regulatorypractices.At present service providers maintain data backup as per their own self regulatory practices for 6 months to a year and thereafter delete/overwrite the data.This is posing major impediment /lacuna in prosecution of cybercrime cases.

## 5. No Chairperson appointed for Cyber Appellate Tribunal (CAT) for past 4 years

The I. T. Act, 2000 provides for the establishment of Cyber Appellate Tribunal where appeals from the decisions of an Adjudicating Officer and Controller may be preferred.[7]At present there is one Cyber Appellate Tribunal in India located at New Delhi but no Chairperson has been appointed for the same for the past 4 years and CAT is not functioning. Section 49 establishes composition of the Cyber Appellate Tribunal consisting of a Chairperson and other Members as a Central Government may appoint through notification in the Official Gazette. The selection of Chairperson and Members is required to be made by the Central Government alongwith the Chief Justice of India.No appointment has been made of Chairperson since 2011 when the last chairperson retired.

## 6. No EEE notified by the Central Government yet

[7] Section 48 of the I. T. Act, 2000.

The Central Government is empowered to appoint any department or agency of the Central Government or State Government as Examiner of Electronic Evidence by virtue of Section 79A to provide expert opinion on electronic evidence before any court or authority. So far no EEE has been appointed and notified till date despite the fact that Amendments were made to appoint such authority in 2009.

## 7. Registration Authority to issue licenses to Cyber café not notified

The Cyber Café Rules were passed in 2011 which provide that a mandatory license must be obtained by every cybercafé prior to starting its business. However, Registration Authority has not been notified by the Government in many states and cybercafés continue to function without a license. This poses a major threat as cyber terrorist attacks could be easily carried out through misuse of cyber café. Also despite the fact that rules envisage periodic monitoring of such cafés by police,there is no mechanism implemented to monitor their functioning including checking maintenance of register of Identity records of persons who use their services and required submission of logs of data to Registration Authority.

## 8. Understanding and deploying Technical measures, particularly to combat heinous crimes such as child pornography and need for strengthening legal framework

Since cyber crimes are committed through use of technology ,understanding the loopholes of technology is very essential to form an effective strategy to combat cyber crimes. Children are viewing so much published adult /child pornographic content on internet which is prohibited in India but accessible from within India and without age verification. In addition, publishing and transmitting obscene content is hit by Section 67,67A and Section 67B( child pornography) of the IT Act,2000. The Author recommends that, it should be made mandatory for Internet service providers to conduct filtering of such sites as a due diligence measure and reporting the illegal activity identified to law enforcement agencies. The Computer Emergency Response Team (CERT) ought to take suo moto action and not only when it receives complaints from Nodal officers or by a court order to block such child pornographic content. The Information

Technology Procedure And Safeguards For Blocking For Access Of Information By Public) Rules 2009 lays down such blocking may be made by CERT for reasons in Section 69A of IT Act to protect India's sovereignty, integrity , but only such sites that contain content injurious to national safety are blocked and complaints of obscene materials are not usually entertained by CERT. Thus, either a police complaint is lodged or ISP is contacted for blocking such sites or a court order is required and no proactive action is suomoto adopted by ISPs (on mandatory basis) or by CERT in this respect.

In order to combat child pornography a mandatory obligation must be put on Internet service providers/ credit card companies to report cases/incidents of browsing/publishing/circulation/sale and purchase of child pornographic content.In addition, free child protection software may be distributed to parents, educators , child care centers, and other relevant institutions by the Government to combat child pornography. Implementation of POCSO Act also has many lacunae such as appointment of Public prosecutors and establishment of adequate courts to deal with child exploitation cases needs to be still put in place. Even otherwise,adequate training of law enforcement personnel is required and greater cyber awareness is required across the general masses to combatcyber crimes.

## 9. Importance of drafting cyber forensic manual and training programmes for law enforcement officers

Due emphasis ought to be given to training personnel in cyber forensics to enable collection, storage and analysis of digital evidence which is legally admissible in a court of law. Also standardization of tools, software, practice of collection and preservation of e-evidence should be prescribed by concerned authorities in form of Notified tools/software &updated Manual for cyber forensics needs to be notified respectively.The office of EEE ( Examiner of Electronic Evidence) should be set up in every state for rendering expert opinions on digital evidence to assist in criminal prosecution in cybercrime matters. As on the date of writing Central Government is yet to notify the cyber forensic labs that will function as EEE under Section 79A of the IT Act,2000.Also, no softwares have been notified to be legally valid software for collection , storage and preservation of electronic data. Specialisedcyberlaws training courses

must be organised by Academies for imparting cybereducation and training to the respective law enforcement agency officers on scheduled basis.

## 10. Need for additional laws to address new emerging issues of cyberspace

Clear laws to address new challenges such as corporate espionage, behavioral advertising and employee surveillance practices requires serious deliberation. For protection of consumers, no law declares what is the basic information that must be provided to a consumer to form a valid e-contract in the form of terms of use on the websites.In order to protect privacy, the Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules, 2011 mandate an e-tailer to have a privacy policy, however neither right of retention and /or print of e-contract is addressed therein nor basic disclosure of terms to form a valid e-contract has been prescribed. Except Section 42, in the IT Act,2000 that puts every subscriber under an obligation to maintain control over its private key of a digital signature,there are other no specific provisions under the Act to deal with problems of loss of passwords, obligation of a user to format computers and cell phones before they are discarded by individuals. These resources may contain sensitive personal information which are often misused to commit cybercrimes, such as credit card frauds, net banking and ATM frauds.

According to the recent amendments in the IT Act,2000 the Certifying Authorities will now act as repositories of digital signatures. Effective monitoring of its role and creation of a homogenous streamlined online secure system with database of electronic signatures issued by various certifying authorities is a new challenge. Challenge is also with regards to maintaining privacy of digital signatures, and tracing of electronic signature defaulters and prevention of impersonation and identity theft frauds**.**The use of 3G technology, cloud computing, launch of UID and DNA fingerprints in cyberspace will bring forth new challenges in preserving privacy and combating cybercrimes in cyberspace. The concept of cloud computing gives rise to many pertinent legal issues such as the protection of right of privacy, data chain authentication, security, and liability of intermediaries, and jurisdiction and legal enforcement issues. It encompasses issues of determining substantive law, criminality jurisdiction, and application of conflict of law principles too. Another challenge is the issue of multi-tenancy as in a public cloud

different people may have licence to use shared resources in a cloud.Adequate provisions to deal with these challenges will require insertion in the IT Act, 2000. Considering views and suggestions of Legaland technical experts on cyberlaws will contribute to framing effective cyber regulations and strategic policies for effective legal framework to combat cybercrimes in India [8].

## 11. Need for law of convergence

There is also an imperative need for law of convergence in India. In case of unauthorised interception found on landline network , TRAI has its set of laws and internal policy for phone tapping. In case of mobile phones interception, the Ministry of Information Technology guidelines and Rules under IT Act, 2000 also apply because IT Act applies to Internet and communication devices [9]such as cell phones. In the case of fixed telephone network, the Central Government and State Government are empowered to intercept phones under section 5 of the Indian Telegraph Act, 1885. In the *PUCL*[10] case, the Supreme Court elucidated clear guidelines for phone tapping which was permitted only where there was reasonable suspicion of illegal activity for reasons recorded in writing. The Supreme court held that the right to protect privacy is a fundamental right under Article 21 of the Indian Constitution and laid down that such phone tapping requires permission from the home secretary from the Central Government and State Government. It is important to note that although Section 69 of the IT Act, 2000 designates the same authority to approve interception request[11] , however in case of emergencies the head and senior most officer could grant and approve at Central level or at state level an officer not below Inspector General of Police (IGP) could allow interception, and

[8] Karnika Seth, **"**Strategies For Enforcement Of Cyberlaws"**,**High Level Consultation Meeting for formulation of a National Policy and Action plan for Enforcement of Cyberlaw , NALSA & AP SLSA, 21-22 May , 2011, and see Seth , Karnika , 'Strategies For Enforcement Of Cyberlaws',High Level Consultation Meeting for Formulation Of A National Policy and Action Plan For Enforcement of Cyberlaw , Maharashtra Judicial Academy, 18 19 December , 2010

[9] Section 2 (1 (ha)) of IT Act, 2000 defines a 'communication device' and includes a cell phone in its definition

[10]PUCL V UOI, (1986) (9) SCALE

[11] The Information Technology (Procedure And Safeguards For Interception, Monitoring And Decryption Of Information ) Rules, 2009

later send it for approval of competent authority within 3 days. In case of landlines, in an emergency case the power could be delegated to officer of the Home Department of Government of India and State Government, not below the rank of joint secretary and the copy of such order is required to be send to the Review Committee within one week from the of issuance of the order. Hence, there are practical differences in internal policy for interception as regard landline and cell phones under IT Act. Whereas under the Telegraph Act,the concerned authority could pass an order for interception not only when necessary in the interest of sovereignty and integrity of India, security of state, friendly relation with foreign states, public order or preventing incitement for commission of an offence, Section 69 of the IT Act, 2000 goes further beyond Section 5 of Telegraph Act and allows interception even to 'investigate any offence'.

At present the rule and policy making of TRAI and Ministry of IT needs synchronization. For example, TRAI passed the Telecom Commercial Communication Customer Preference Regulation, 2010. As per the Regulations, the customer who do not wish to receive unsolicited tele- marketing calls could register in fully or partially blocked category and a customer could change its preference letter. In order to prevent the misuse of phone number for tele calling or SMS a limit of 200 SMS per day per SIM Card has been provided under these rules. Although unsolicited advertising through fixed lines and cell phones decreased, it led to an increase in the use of internet calling for such activities to circumvent the laws .This explains the growing need to develop and streamline convergence law in India. The Convergence Bill, which was proposed in the year 2000, is yet to be passed. The Bill aims to repeal the Indian Telegraph Act, 1885, The Indian Wireless Telegraph Act, 1933, The Cable Network Regulation Act, 1995, and the Telecom Regulatory Authority of India (TRAI) Act, 1997

## 12. Ambiguity in Section 66A of IT Act,2000

One of the cognizable offence under IT Act is sending offensive messages using a communication service as per Section 66A of IT Act,2000.The meaning and ambit of "offensive messages, or menacing messages " is also unclear and may involve subjective interpretation as it is not defined by the IT Act,2000. This issue is pending before the Hon'ble Supreme court of

India in *Shreya Singhal v UOI*( WP (crl.) 167/2012) . Meaning of "defamation" may also vary from jurisdiction to jurisdiction. Further, Rule 3(2) of the IT ( Intermediaries Guidelines) Rules, 2011 mandates removal of an illegal content posted by a user within 36 hours of complaint by an aggrieved person on various grounds that are not objectively defined by the IT Act or rules and may be misused to breach privacy and freespeech on internet. In particular, the terms such as 'grossly harmful', 'harassing', 'blasphemous', 'hateful' , 'ethnically objectionable' ,' harmful to minors,' are subject to different subjective interpretations just as due diligence standards may vary across jurisdictions. In certain situations such content as described by Rule 3 of IT (Intermediaries Guidelines) 2011,when complained of by an aggrieved person may fall outside purview of Section 69A of IT Act,2000 as it may not have any element or the required degree of seriousness to satisfy ' public order' involved although it may have element of 'incitement to commission of a cognizable offence' under Section 69A.

Also, if government proposes to precensor/pre-filter such third party content, then clear rules that define ambit and scope of such regulation, including due diligence process for pre- filtering by intermediaries ought to be passed[12] and its technical and administrative feasibility also should be considered. It is the suggestion of the Author, that the scope of ambit of terms "harmful to minors", "harassing" "hateful" may be clarified with help of illustrations as found in the Indian Penal Code. For example, on consumer blogs complaining about deficient services of a service provider is protected by free speech so long as it does not use abusive language or becomes defamatory.Thus,the meaning and scope of terms such as "harmful to minors", "harassing" "hateful" can either be clarified by judicial decisions or explained by Parliament through illustrations as in case of Indian Penal Code.

## 13. The IT (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011

One shortcoming of these rules is that it fails to address any compulsory terms of use that the entity should adopt and declare or prior information requirements for making contractual

[12] At present Ministry of IT has clarified that due diligence process as per Internationally accepted standards needs to be observed by all Intermediaries. See Press note " Due diligence to be observed by Intermediaries" , May 14,2011 http://www.mit.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf ( as accessed on 18 April 2012.)

disclosures to a consumer before he requests for an e-commerce service. As a result many customers who shoponline ,often shop on fake website or on terms of service provider that severely prejudice their rights both in relation to merchandise bought and as regards personal information collected by the website.

The said rules also do not clarify issues of privacy protection as regards disclosure in public directories, method of collection via cookies or traffic data. Aspects of unsolicited advertisement and opt in and opt-out procedure have also not been discussed as regards non sensitive personal information. Also, there exists lack of clarity on what information a user can safely post on the internet. As regards to data protection, although Indian Rules provides opt-in approach before a body corporate collects 'sensitive personal information' of netizens , it fails to provide any law regarding consent of a user as to the method/mode of the collection.

## 14. Need for removal of ambiguity as regards power of Adjudicating Authority to grant injunction

Another interesting issue is whether Adjudicating Authority has the power to grant injunction orders under Section 46 of the IT Act, 2000 as interim measure as every adjudicating officer has powers of civil court on Cyber Appellate Tribunal under section 58(2) of IT Act,2000.This only mentions specified powers, summoning and enforcing attendance of any person on oath, requiring discovery and production of documents or electronic records, receiving evidence on affidavits, issuing commissions for examining witnesses or documents, reviewing its decisions, dismissing application for default, or deciding it exparte and any other prescribed matter. It is protected by provisions for contempt of court as any judicial office of civil or criminal court[13].It also has power of execution of its orders after the IT ( Amendment ) Act, 2008.[14]

One argument would be that it has no power to grant interim injunction order because it cannot grant final order of injunction and can only grant damages to a party. The Information

[13] See Section 46 (5) (a), (b) IT Act,2000
[14] Section 46(5)© IT Act,2000

Technology (Qualification and Experience of Adjudicating officers and manner of holding enquiry) Rules , 2003 also does not provide that Adjudicating officer can grant injunction orders. On the other hand , it is arguable that in a Information Technology law case (where issues of copyright law may not be involved) if Adjudicating officer does not have injunction power , Section 61 of IT Act,2000 which bars jurisdiction of civil courts will mean that affected party cannot seek a injunction order from a civil court .This will be injurious and not adequately protect interests of the affected party.

In my view, such a situation is not contemplated by the objectives of the Act and in particular Section 46 of the IT Act, 2000.Therefore, Adjudicating Authority should be deemed to be conferred with power to grant injunction orders in addition to providing compensation.It will be advisable for central government to prescribe by notification that such powers are conferred on the Adjudicating Authority aswell as the Cyber Appellate tribunal. Injunction orders are necessary to restrain continued infringement or violation of law and to avoid irreparable loss that may be caused to a party if such a remedy is not granted at the initial stages, provided a primafacie case exists and balance of convenience is also in favour of the plaintiff. My argument finds support in the language of Section 61 of the IT Act,2000, which bars jurisdiction of civil court to entertain any suit or proceeding in respect of any matter wherein Adjudicating Authority Or Cyber Appellate Tribunal are empowered to determine.It further states '*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*."

## 15.Adopting a sound IT and HR policy

Certain cyber crimes are committed by insiders or hackers and one single strategy may not be a solution for all kinds of crimes. To combat crimes dealing with insiders, an effective Human Resource and IT Policy will be indispensible, clear standing orders on use of computer technology by employees and clear policy on employee surveillance measures within organizations are also necessary steps.Infact, it should be made mandatory as per the IT Act,2000 that every organization ought to have a well defined IT Policy in place. The practice of employing variations with ways to prevent employees' frustration within organisation and

providing a conducive programme for employees' growth and training can curtail insider frauds with some psychological management.

Every organization needs to install reasonable security parameters such as fire walls, anti-virus software and put in place an incident response plan to safeguard the organizations from cyber crimes. The recent rules, Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules 2011 for reasonable security practices mandate ISO27001 or other approved standards to be implemented by all body corporates. The backup systems must be strong enough to have continuous backup arrangements for storing sensitive data and upgrading of hardware and software as per industry practice. Digital signatures can be useful in preventing cyber crimes within an organisation and other encryption techniques can help in maintaining integrity of data being transmitted across the computer networks. Safeguards for preserving computer and network security is a pre-requisite for any organisation and creation of secured zones is recommended[15].Continuous developments in building secure computer networks and cybersecurity devices should be encouraged. Cyber Awareness workshops for employees will also be vital in preventing cybercrimes. An effective public private partnership in combating cybercrime may be a positive step.

## 16.Spreading awareness to combat cybercrimes

An important first step to curtail rise in cybercrimes is to educate the people about their rights and obligations in cyberspace and legal remedies in cyberspace law.Conducting cyberlaws workshops in Schools and Colleges should be made mandatory as part of their curriculum , particularly for senior secondary schools as children between age group 11-17 use Internet for Social networking , for academic assignments or otherwise.

A large number of cybercrimes are caused due to misuse of internet banking facilities by cybercriminals or by ATM or credit card frauds. Therefore, it should be made compulsory for

[15] For instance, Honey Pots help in identifying any intrusion attacks.

banks to hold cyber awareness workshops, set up a helpline and cyber cell to educate its customers on protecting their passwords and sensitive information online, reporting frauds and making its customers aware of their rights and remedies in case they become victims of cybercrime. Using visual demonstrations of how ATM frauds are perpetrating and displaying do's and don't's of internet banking through CDs will have more impact on customers rather than merely providing written information . Banks also need to cooperate with investigation agencies to investigate cyber frauds and also the banks need to strengthen KYC and other internal processing norms for e-banking to prevent cyber crimes.

Nasscom and other bodies, including Internet Service providers, Chambers of commerce and consumer protection organisations need to hold seminars to educate people on maintaining best security practices and netiquettes while transacting business or communicating online .It should also inform its members on launch of new software products and tools for enhancing cybersafety , and send alerts on imminent threats in cyberspace through sms or other means to members/subscribers who may subscribe to such information updates from these bodies.

The cybercrime alerts from Police departments, CERT,NIA,NASSCOM must be mandatorily published in such newspapers from time to time so that the general public is aware of imminent or existing dangers of transacting online such as through virus attacks or Nigerian or phishing scams and the general public may adopt suggested precautions for Internet safety. Since most victims report criminal matters such as fraud and cheating cases to the Police, it is important for Police stations to have a cyber crime cell in each district to educate the victims of cyberfrauds about their civil rights to claim compensation before the Adjudicating Authority. In many police stations, FIR are not yet registered online and it will only increase reporting of crime if police stations are well equipped with computers and internet and police personnel are imparted training in information technology and laws related therewith.

**Drawn on: 12 Dec 2014**

by-

**Karnika Seth**

Cyber law expert, and Advocate, Supreme Court of India

Visiting Faculty, NIA, CBI, National Police Academy and National Judicial academy

Author of *'Computers, Internet & New Technology Laws'*, 2012 , Lexis Nexis

**Contact details**

*Office address*- Seth Associates, Advocates & legal consultants

B-10 Sector 40, NOIDA-201301

*Mobile*: 9810155766

*Office*: 01204352846

*e-mail*: karnika@sethassociates.com

*****END OF DOCUMENT*****