INDIAN CYBERLAW ON CYBERCRIMES

Mr. Pavan Duggal*

India is on the move. As the nation is progressing, there are numerous changes that are happening in the legal regime regulation Information Technology in India.

There have been certain important changes that have been made in the existing information technology legislation in our country. These changes are particularly important since they impact all companies using computers, computer systems, computer networks, communication devices as well as data and information in the electronic form.[1]

The Information Technology Amendment Bill, 2008 was passed by the Lok Sabha and the Rajya Sabha in December, 2008 and the said amendments came into effect from 27th October, 2009.[2] Sweeping changes have been made in the existing Indian cyber law, namely the Information Technology Act, 2000.[3]

The Information Technology Act, 2000[4] (hereinafter the IT Act, 2000) is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. The said legislation has provided for the legality of the electronic format as well as electronic contracts. This legislation has touched varied aspects pertaining to electronic authentication, digital signatures, cybercrimes and liability of network service providers.

---

* Advocate, Supreme Court of India; President, cyberlaws.net; President, Cyber Law Asia; Head, Pavan Duggal Associates.
The author Pavan Duggal is Asia's and India's leading expert and authority on Cyberlaw and Mobile Law. He can be contacted at his email addresses pavan@pavanduggal.net and pavanduggal@yahoo.com. More about the Author is available at www.pavanduggal.net and http://www.linkedin.com/in/pavanduggal.

1 Pavan Duggal, *Section 66(A) of the Information Technology (IT) Act*, IBNLIVE (Dec. 3, 2012), http://ibnlive.in.com/chat/pavan-duggal/section-66-a-of-the-information-technology-it-act/1328.html (last visited July 5, 2014).

2 PAVAN DUGGAL, MOBILE LAW 310 (2nd ed., Universal 2013).

3 *Id.* at 153.

4 Padmaja Joshi, *Reading 'The Satanic Verses' Not a Punishable Offence, Say Legal Experts*, INDIA TODAY (Jan. 24, 2012), http://indiatoday.intoday.in/story/salman-rushdie-the-satanic-verses-jaipur-authors-legal-experts/1/170439.html (last visited July 5, 2014).

From 17th October, 2000, when the IT Act, 2000 came into implementation till date, the said legislation has seen some very interesting cases and challenges, being brought within its ambit. As time passed by, the inadequacies of the said legislation came to the forefront. There were various practical difficulties in the implementation of the said legislation.[5] The inadequacy[6] of the IT Act, 2000 to address some of the emerging phenomena, challenges and cybercrimes, led to voices clamoring for change in the Indian cyber law.

Consequently, the Government of India tabled the Information Technology Amendment Bill, 2006 before both the houses of Parliament in December, 2006, which referred the said amendment bill to the Parliamentary Standing Committee on Information Technology. The Parliamentary Standing Committee examined the amendments in a comprehensive manner and thereafter gave its report and recommendations thereon.

Due credit needs to be given to the government, for removing the various practical difficulties of the IT Act, 2000.[7]

The lawmakers and the Government have to be complemented for their appreciable work removing various deficiencies in the Indian cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation, more so on corporate India.

A careful analysis of the said amendments, clearly bring home the point that the 2008 amendments to the IT Act, 2000 are not at all sufficient in the context of emergent needs of corporate India and have various glaring loopholes.

The issues relating to confidential information and data of corporates and their adequate protection have not been adequately

---

5 Samanwaya Rautray, *IIPM Case Clear Abuse of Judicial Process, Say Legal Experts*, THE ECONOMIC TIMES (21 Feb. 21, 2013), http://articles.economictimes.indiatimes.com/2013-02-21/news/37221838_1_injunction-iipm-urls (last visited July 5, 2014.

6 Pavan Duggal, *Indian Cyberlaw in 2008*, CYBERLAW TRENDS OF 2010 (Dec. 31 2008) http://cyberlawindia2008.blogspot.in/2008/12/indian-cyberlaw-in-2008.html (last visited July 5, 2014).

7 Pavan Duggal, *Glaring Loopholes in Cyberlaw Amendments (2008) Oct.-Dec.* INFOTECH, http://inclusion.in/index.php?option=com_content&view=article&id=193:glaring-loopholes-in-cyberlaw-amendments&catid=114:infotech (last visited July 5, 2014).

addressed.[8] The said law is not a comprehensive law on data protection or on digital secrets. Having a couple of sections on data protection does not serve the requirements of corporate India.[9]

India has neither learnt from the wisdom of the United States nor the European Union, in terms of their respective experiences, in the area of data protection. The provisions will not aid the victim entities, whose data and information is often misused by their employees or agents with impunity.[10]

The IT Act Amendments are also deficient in the sense that they do not create rebuttable presumptions of confidentiality of trade-secrets and information, in the context of corporate India. A large number of Indian companies and individuals are saving their confidential data, information and trade-secrets in the electronic form on their computers.[11] Given the apparent increase in technology adoption, it is increasingly being found that that despite all precautions been taken, the employees are still going ahead and taking away confidential data from companies. The inability of the law to create enabling presumptions of confidentiality regarding corporate and individual data and information in the electronic form, is likely to complicate matters further for Indian companies and netizens.

Given the move to take an extremely lenient view on most cybercrimes, corporates need to forget about being able to get their errant employees, misusing their confidential data and information, behind bars. Absence of an effective remedy for corporates by the 2008 amendments to the Information Technology Act, 2000 is likely to further erode the confidence of the Industry in the new cyber legal regime. The maximum damages by way of compensation stipulated by the cyber law amendments is Rs.5 *crore*. When calculated in U.S.A. Dollar terms, this is a small figure and hardly provides any effective relief to corporates, whose confidential information worth *crores* is stolen or misused by its employees or agents.

Another major failure of the amendments is that they have not dealt with the entire issue pertaining to spam, in a comprehensive manner.[12] In case, the word 'spam' is not even mentioned anywhere in the IT Amendment Act passed by both the houses of the

---

8 Pavan Duggal, *Legal Issues Relating to Outsourcing in India*, (2008) 36 (2) IJLI 369.
9 *Id.*
10 Pavan Duggal, *We're Not Keeping Pace*, THE TIMES OF INDIA (Jan. 29, 2009), http://timesofindia.indiatimes.com/home/opinion/edit-page/TOP-ARTICLE-Were-Not-Keeping-Pace/articleshow/4043106.cms (last visited July 5, 2014).
11 DUGGAL, *supra* note 6.
12 PAVAN DUGGAL, TEXTBOOK ON CYBER LAW 60 (1st ed., Universal 2014).

Parliament. India has missed yet another opportunity to deal with the contentious issue of spam.[13]

It is pertinent to note that the countries like U.S.A., Australia and New Zealand have demonstrated their intentions to fight against spam by coming across with dedicated anti-spam legislations.[14] However, in India, we neither have any anti-spam legislation, nor we have any specific provisions for effective prevention and regulation of spam. This make India a heaven as far as, spam is concerned. This is all the more serious since India already features in the top ten nations of the world from where spam originates.

Any major failure of the IT Act Amendments is that they have not specifically detailed with the issues pertaining to electronic discovery.[15] Today, increasingly people and entities as also corporates are relying upon electronic evidence and electronic media as a means of communicating with each other and doing business.[16] However, the Indian IT Act Amendments are completely silent on the issues of electronic discovery. This once again shows the short sightedness of the Indian IT Amendments to address the complicated emerging issues pertaining to electronic discovery.

The IT Act amendments do not address jurisdictional issues17. At a time when the Internet has made geography history, it was expected that the 2008 amendments to the Information Technology Act, 2000 would throw far more clarity on complicated issues pertaining to jurisdiction. This is because numerous activities on the internet take place in different jurisdictions and that there is a need for enabling the Indian authorities to assume enabling jurisdiction over data and information impacting India, in a more comprehensive way than in the manner as sketchily provided under the current law.

The amendments to the Information Technology Act, 2000 make it mandatory for corporates, possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices, and procedures. It has to be pointed out that one set of security practices will not fit the entire nation. What would be reasonable security practices for one industry

---

13 *Id.* at 60-61.

14 *More Teeth and Byte to IT Law*, THE HINDU (Business Line, Nov. 9, 2009), http://www.thehindubusinessline.com/todays-paper/more-teeth-and-byte-to-it-law/article1084553.ece (last visited July 5, 2014).

15 DUGGAL, *supra* note 6.

16 DUGGAL, *supra* note 12, at 73-76.

17 Shashank Pandey, *Not by Proxy*, NEWSLAUNDRY (June 14, 2014), <http://www.newslaundry.com/2014/06/14/not-by-proxy/ (last visited July 5, 2014).

may not be directly applicable to another industry. Non-maintaining such reasonable security practices, would expose the said corporates to civil liability to pay damages by way of compensation to the person so affected, to the tune of Rs.5 *crore*. The amendments to the Information Technology Act, 2000 are likely to impact all industries, which use computers, computer systems and computer networks and data and information in the electronic form. These reasonable security practices and their mandatory adoption, while in overall better interests, are likely to unveil a package of unpleasant surprises for many.

The most startling aspect of the amendments to the IT Act, 2000 is that these amendments have had the effect of transforming the Indian cyber law into a cyber crime friendly legislation-a legislation that goes extremely soft on cyber criminals, with a soft heart[18]; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment[19] accorded to them under the existing law; a legislation that chooses to give far more freedom to cyber criminals than the existing legislation envisages; a legislation which actually paves the way for cyber criminals to wipe out the electronic trails and electronic evidence by granting them bail as a matter of right; a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences[20]; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world.

A perusal of the said legislation shows that there is hardly any logical or rational reason for adopting such an approach.

However what amazes the lay reader is that the amendments to the IT Act have gone ahead and reduced the quantum of punishment. Taking a classical case of the offence of online obscenity, Section 67 has reduced the quantum of punishment on first conviction for publishing, transmitting or causing to be published any information in the electronic form, which is lascivious, from the existing 5 years to 3 years. Similarly, the quantum of punishment for the offence of failure to comply with the directions of the Controller of Certifying Authorities is reduced from 3 years to 2 years.

Further, it is shocking to find that the existing language of the offence of hacking under Section 66 has now been substituted by new language. Deleting hacking as a specific defined offence does not

---

18 HINDU, *supra* note 14.

19 Pavan Duggal, *Your Cybercrime-Friendly Legislation*, BUSINESS-STANDARD (Jan. 8, 2009), http://www.business-standard.com/article/technology/your-cybercrime-friendly-legislation-109010801070_1.html (last visited July 5, 2014).

20 DUGGAL, *supra* note 12, at 110.

appeal to any logic. The cutting of certain elements of the offence of hacking under the existing Section 66[21] and putting the same under Section 43 make no legal or pragmatic sense. This is all the more so as no person would normally diminish the value and utility of any information residing in a computer resource or affect the same injuriously by any means, with the permission of the owner or any such person who is in charge of the computer, computer system or computer network.

At that time when the entire world is going hammer and tongs against cyber crimes and cyber criminals, here comes a contrary trend from the Indian legislature.[22] Cyber criminals of the world targeting India or operating in India need not despair. The legislation has now stipulated that cyber crimes punishable with imprisonment of 3 years shall be bailable offences. Since the majority of cyber crime offences defined under the amended IT Act is punishable with 3 years[23], the net effect of all amendments is that a majority of these cyber crimes shall be bailable. In common language, this means that the moment a cyber criminal will be arrested by the police, barring a few offences, in almost all other cyber crimes, he shall be released on bail as a matter of right, by the police, there and then.[24]

Keeping in account human behavior and psychology, it will be but natural to expect that the concerned cyber criminal, once released on bail, will immediately go and evaporate, destroy or delete all electronic traces and trails of his having committed any cyber crime, thus making the job of law enforcement agencies to have cyber crime convictions, a near impossibility.

The fertile liberal treatment meted out to cyber criminals, by the IT Act amendments, facilitating the environment where they can tamper with, destroy and delete electronic evidence[25], is likely to make a mockery of the process of law and would put the law enforcement agencies under extreme pressure, apart from exposing corporates to undesirable headaches. In the 14 odd years since internet have been commercially introduced in our country, India has got only three cyber crime convictions. Since the coming into effect of the amendments, India has seen a drought of cyber crime convictions.

---

22 DUGGAL, *supra* note 17.
23 DUGGAL, *supra* note 12, at 111-139.
24 DUGGAL, *supra* note 17.
25 Rishi Raj, *Satyam Records Not Yet Seized*, THE FINANCIAL EXPRESS (Jan. 9, 2009), http://www.financialexpress.com/story-print/408405 (last visited July 5, 2014).

Another major change that the amendments to the IT Act, 2000 have done is that cyber crimes in India shall now be investigated not by a Deputy Superintendent of Police, as under the existing law, but shall now be done by a low level police inspector. So, henceforth, the local police inspector is going to be the next point of contact, the moment a person or any company is a victim of any cyber crime. The efficacy of such an approach is hardly likely to withstand the test of time, given the current non-exposure and lack of training of Inspector level police officers to cyber crimes, their detection, investigation and prosecution.

Given this new development, it is probable that the concept of *e-hafta* (or electronic *hafta* is likely to be far more reinforced and developed as an institutional practice. This is so as the law has now produced more powers to the inspector than ever before, regarding cybercrimes.

The expectations of the nation for effectively tackling cyber crime and stringently punishing cyber criminals have all been let down by the extremely liberal amendments, given their soft corner and indulgence for cyber criminals.

The entire issue relating to encryption as a process, has not been satisfactorily dealt with. Having a single provision in the 2008 amendments to the IT Act, 2000, reserving the right to specify processes relating to encryption later, does not do justice to the expectations of corporate India, regarding the usage of encryption.

Encryption is a process that scrambles information, such that it cannot easily be understood by people who do not have the right key to unscramble it. The level of security this provides depends critically on the length of the keys used in the encryption and decryption process. The maximum permissible length of this key has been a matter of debate, discussion and dispute between the technology industry and the government. The implications of this are highly significant for commerce, law, intellectual property protection, and civil liberties.

Rather than addressing the complicated issues of encryption and defining a comprehensive policy on encryption, the amendments have merely decided to defer the said issue and leave it to the route of secondary legislation by means of rules and regulations. This makes the situation all the more complicated, given the existing position.

India's Guidelines and General Information for Setting up of International Gateways for Internet and similar documents stipulate

that "encryption up to 40-bit key length in the RSA algorithms or its equivalent in other algorithms can be used without having to obtain permission. If encryption equipments higher than this limit are to be deployed, it needs permission of the Telecom Authority and deposit the decryption key, split into two parts, with the Telecom Authority."

The practical problem is that encryption upto 40 bits of length is absurdly easy to crack, even by schoolboys. Today, banks and financial institutions are openly violating the official limit of 40 bit encryption. At a time, when the world is moving towards one direction, India should not be seen to be moving in the opposite direction.

India needs to harness the benefits and advantages of technology, rather than wanting to ride its boat upstream, against the current of the technological river.

All in all, given the glaring loopholes as detailed above, the IT Act Amendments have already had the effect of adversely impacting corporate India and all users of computers, computer systems and computer networks, as also data and information in the electronic form.

In conclusion, it can be safely stated that the changes that are brought about by the Information Technology Act, 2000 by the 2008 amendments are the law of the land. Till such time as the said law is not freshly amended, companies using computers, computer systems, computer networks, communication devices as well as data and information in the electronic form, will need to ensure compliance with the same. Due diligence in the electronic environment is the main message that the IT Act amendments have for corporates. All corporates using computers, computer systems, computer networks, communication devices as well as data and information in the electronic form, must ensure that their electronic operations are in compliance with the existing cyber law. Compliance, compliance and compliance are the key messages that corporates in India need to concentrate upon, for the present.

INTRODUCTION TO CYBERCRIME AND PROCEDURE TO REPORT CYBERCRIME

Mr. S.M. Babar*

Cybercrime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. This includes offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim, or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Computer crime encompasses a broad range of activities.

* Senior Police Inspector, Market Yard Police Station, Pune City.

General	**Computer as a target**	**Computer as a tool**	**Intellectual property crimes**
1.Cyber terrorism	**1.**Computer viruses	**1.**Fraud and identity theft	**1.**Software piracy-illegal copying of programs, distribution of copies of software
2.Cyber extortion	**2.**Denial-of-service attacks	**2.**Information warfare	**2.**Copyright infringement
3.Cyber warfare	**3.**Distributed denial of service attacks	**3.**Phishing scams	**3.**Trademarks violations
4.Obscene or offensive content	**4.**Malware	**4.**Vishing	**4.**Theft of computer source code
5.Harassment & Cyber stalking		**5.**Spam	**5.**Internet time theft
6.Threats		**6.**Propagation of illegal obscene or offensive content, including harassment and threats	
7.Drug trafficking		**7.**Cyber defamation	
8.Credit card fraud			

Crime against organization	**International level**	**National level**	**Individual level**
1.Unauthorized accessing of computer	**1.**Anonymous use of ICTs for attacks on critical infrastructure	**1.**Attacks on critical infrastructure	**1.**Social engineering
2.Denial of service	**2.**Botnets	**2.**Web defacements	**2.**Email hacking and Misuse
3.Computer contamination/Virus attack		**3.**Website intrusion and malware propagation	**3.**Abuse through emails
4.Email bombing		**4.**Malicious code and spread of botnets	**4.**Abuse through social networking sites
5.Salami attack		**5.**Scanning and probing for cyber espionage	**5.**Laptop theft
6.Logic bomb			
7.Trojan horse			
8.Data diddling			

9.Domain stalking			
10. Scanning and probing			
11. Insider threats			

Procedure to Report Cyber Crime

To tackle the issue of cyber crimes, CIDs (Criminal Investigation Departments) of various cities opened up Cyber Crime Cells in different cities. The Information Technology Act of India, 2000 states clearly that when a cyber crime has been committed, it has a global jurisdiction under Section 1(2). Hence a complaint can be filed at any cyber cell as well as it can be registered at the place where it is disclosed/happened.

Step 1-One may need to provide name, mailing address and telephone number along with an application letter addressing the head of a Cyber Crime Investigation Cell, Police Stations when filing a complaint.

Step 2-One must provide certain documents in order to register a complaint. List of documents varies with the type of cyber crime.

In case of hacking the following information should be provided:

1) Server logs.
2) A copy of the defaced web page in soft copy as well as hard copy format, if victim's website is defaced. If data are compromised on victim's server or computer or any other
3) network equipment, soft copy of original data and soft copy of compromised data.
4) Access control mechanism details i.e., who had the access to the computer or email of the victim?
5) List of suspects if the victim is having any suspicion on anyone.
6) All relevant information leading to the answers to following questions.
   - What is compromised?
   - Who might have compromised the system?
   - When was the system compromised?
   - Why might have been the system compromised?

- Where is the impact of the attack-identifying the target system from the network?
- How many systems have been compromised by the attack?

In case of e-mail abuse, vulgar e-mail etc., the following information should be provided:
1) The extended headers of offending e-mail.
2) The offending e-mail from.

Adjudicating officer is Secretary to IT department Maharashtra State. He has the powers to make orders for compensation up to Rs.5 *crores* after deciding who is in lapse in the cases of monitory loss, intellectual loss under Section 43.

Contact Information of Cyber Cells, Pune:
Cyber Crime Investigation Cell
Deputy Commissioner of Police (Crime)
Office of Commissioner Office,
2, Sadhu Vaswani Road,
Camp, Pune-411001

Police Helpline Numbers: +91-20-26123346, +91-20-26127277, +91-20-2616 5396, +91-20-2612 8105 (Fax)
Website: www.punepolice.gov.in
E-Mail: crimecomp.pune@nic.in,

Contact Information of Cyber Cells, Mumbai:
Cyber Crime Investigation Cell
Office of Commissioner of Police Office,
Annex-3 Building,
1st Floor, Near Crawford Market,
Mumbai-01.

Police Helpline Numbers: +91-22-22630829, +91-22-22641261
Web site: http://www.cybercellmumbai.com
E-mail: officer@cybercellmumbai.com

SOME BASIC RULES FOR SAFE OPERATIONS OF THE COMPUTER AND INTERNET

Ms. Vaishali Bhagwat*

Introduction

Today we are living in a completely wired world and with the convergence of technologies life is getting simpler (or complex one wonders). With convergence of technologies, I mean that your wristwatch is no longer just a strap on your wrist which shows time but a camera, recorder, music player, GPS, data storage, all into one. Your washing machine at home can also answer door bell and let the courier man in, but keep the burglar out.

Don't be too surprised! This day is not far away. We are left with no choice; we have to keep up with technology or become obsolete or useless.

Today you walk inside any shop, mall, multiplex, petrol station and you don't need paper money to do the transactions, but only plastic which is your credit card or debit card or any other smart card. Just a swipe of the card and the shopping is done; the money is debited or minused from your bank which could be situated anywhere in the world almost immediately and you get a SMS alert almost the next instant. The money gets deposited in account of the shop owner, again electronically. So where is all the money that we are using while doing the shopping? It's all there on some computer somewhere in the world which you are assuming is well protected and all your money is safe.

Just imagine how big the risk is if such transactions are not carried out carefully or not monitored carefully. Someone may have created your profile on *Orkut* and must be communicating with your friends all over the city, country or the world, and people are talking to the person as if 'he' is 'you'. That's scary, right? Someone may also create an email id by your name and start sending dirty messages/pictures to your friends.

Does this mean you should stop using the internet or computers? Now that is no longer possible; so it is better that we learn how to use it safely and protect ourselves. It is also important to know that while

* B.Sc.,LL.B.Practising Cyber Lawyer, Pune;TCS Chevening Scholar.

using the computer and internet, you should follow certain rules, regulations, laws and guidelines because if you do not do that, it may be an offence punishable under law. The way we follow traffic rules while driving on the road, it is the same while using the internet.

Let us first begin with discussing what are those few wrong beliefs or myths about using the computer and internet.

Myth No.1: Because it is technologically possible, it is legal.

Reality: Not legal!

It may be easily possible to break into somebody's email account or access the email account without authority. It is also easily possible to cut-paste photographs and images you like that are available on different websites on to your own website or blog. Making changes in the photographs or pictures of people on the internet (also called as morphing). But that is not legal. You cannot access somebody's email account without the person's permission. You cannot cut-paste photographs and images available on the internet without the owner's permission. You cannot make changes in photographs.

Myth No.2: Because the information is available on the internet is free.

Reality: No!

All information available on the internet belongs to the creator or author of the information. It could be contents of a website, a picture, drawing, music, and video. You cannot simply copy it and use it unless the website gives you permission to do that. You thought downloading music or videos from the internet is right, right? Think again! If the creator or publisher of the music or video has not given rights of free distribution, you may be committing an offence.

Myth No.3: Information available on the website is always true and correct.

Reality: Now this is a funny one!

Take *Wikipedia* for example. It has information that is posted by users like you on me. Information on websites is put there by creators of the website who may not be always correct. Content could be the author's perception or view about a certain topic or written out of his limited knowledge. Check the source of the information before relying on it would be my advice.

Myth No.4: Internet of offers you anonymity. No one knows who you are on internet.

…Which means you can do whatever you want on the internet. Send dirty jokes, dirty SMS etc. to people; threaten or defame people on blog sites or twitter or elsewhere; talk to people on chat under false identity because no one will know who you actually are.

Reality: A big NO to this!

Remember, every time you touch the keyboard, you are creating a footprint which cannot be wiped away. Whenever you send an email from your computer, it will carry the physical address of the computer which means the place from which the email was sent or the chat conversation was done can be very easily found out. It could be your home, school, college, office or a cyber cafe. After that finding a person who has sent it is not so difficult.

Internet gives you a false sense of anonymity or security because you are faceless. That automatically gives you some extra courage and strength to do things that you otherwise would not do, such as-chatting in a dirty language, posing to be a handsome 23 year old boy or a beautiful 16 year old girl on the internet when your age is actually 65. Why? Because you feel no one is watching. Think again! The law is watching and it is very easy to trace footprints on the net, easier that the physical world.

Myth No.5: Usage of internet is not governed by any rules, regulations or laws; you can do what you want.

Reality: No!

And that is why Rotary Club along with Pune Police has organized this awareness drive.

Seven Rules for Safe Operations of Computer and Internet

1	**Rule 1**	Use licensed software.
2	**Rule 2**	Use antivirus software.
3	**Rule 3**	Use a firewall.
4	**Rule 4**	Protect your password.
5	**Rule 5**	Do not operate under a false identity.

6	**Rule 6**	Maintain decency and decorum on public websites.
7	**Rule 7**	Use common sense and be alert.

Rule 1: Use only licensed software.

Why? Because by not doing so you are committing a crime punishable with imprisonment and fine. The police officers can also seize the computer on which pirated software, music, video is loaded.

A software manufacturer permits a user to use the software on payment of a fee, called the license fee. On such payment the user is also entitled to updates that keeps the software running in good condition and also makes your computer safe and secure. If one does not want to purchase a software other option like free software are also available called as 'open source' software.

Cracking the license of a software so that multiple copies can be made is also a crime.

Rule 2: Install agood antivirus software on your computer and keep it updated regularly.

Virus, Worms, Torjans etc., are those germs which infect a computer and can cause damage to the computer and data making it useless. Valuable data can be lost forever. Virus etc., can enter into your computer through the internet or even through floppy disks, USB drives etc. In order to protect your computer from the virus attack, one needs to install a program on the computer which will prevent the entry of the virus. Such programs are called anti-virus programs.

Rule 3: Install a personal firewall on your computer.

A firewall is program that will protect your computer from offensive websites and potential hackers. A firewall will filter the information entering into your computer and therefore you can filter offensive and 'dirty' pornographic websites thus making your computer use safe, clean and secure. It can also prevent hacking attacks which means stop an unauthorized user using your computer.

Rule 4: Protect your password.

This is easier said than done. How many times you must have already heard this? Let us ask a simple question to ourselves. How many

keys do you have to your house? 1-2-3? Mom, dad and yourself? Do you freely make duplicates and keep them lying everywhere-like on the door itself, on the door mat, in the plant pot outside the main door? No! Isn't it? We are more careful because the house contains lot of valuables.

It is the same with passwords. If you don't protect them, then people are going to misuse them and use them to steal money, data, even your identity. Imagine if someone knows the password to your email account, he may communicate with all your friends on the friend list as you and cause embarrassment.

Password is also sometimes referred to as pin, authentication id, etc.

It means that you should never:

1. Share your password with anyone.
2. Write down the password anywhere.
3. Call out or say your password in a conversation.
4. Allow anyone to see you typing your password.
5. Give your password over telephone while doing any banking or other financial transactions.
6. Do not include personal details in your password–such as family name, spouse name, children name, phone no, birth date, vehicle number etc.
7. Never leave your computer unattended.
8. Do not do internet banking transactions from cyber cafes or other public places.
9. Always systematically log out of the website you have logged in.
10. Be careful, alert and wise.

Rule 5: Do not operate on the internet under a false identity.

Posing of someone else on the internet is a crime punishable with imprisonment and fine. It is also referred to as identity theft. There are several ways in which this is done. For e.g., someone steals your password and starts operating your account without your permission; or someone creates your profile on *Orkut*, *Facebook*, *Myspace* etc.; uploads your pictures and actually starts communicating with everybody as if it's you.

Internet is a powerful medium, but it also gives a false sense to the user that he is faceless and that his identity cannot be known. However this is just a myth. It is very easy to trace the user to his physical address.

Rule 6: Maintain decency and decorum on public chat sites or social networking site.

Pornography is banned in India. Viewing, publishing or transmission of content which is obscene, pornographic, sexually explicit or 'dirty' is a crime in India punishable with imprisonment upto 5 years. Sending dirty text, email, SMS, MMS is a crime.

Also posting content on websites or social networking sites which is offensive, insulting, intimidating or defamatory is also a crime. Be careful of what you write on the internet. Think twice! Because once you write it, you cannot erase it.

Rule 7: Be alert and use common sense.

Have you seen anyone win a lottery without buying a lottery ticket? Then why believe all the emails and SMS that that tell you that you have won a lottery worth million pounds in UK.

The easiest way is-ignore these emails! Be alert!

The Information Technology Act, 2000 was enacted in the year 2000 with the basic objective to make electronic records admissible in evidence, facilitate *e*-commerce, give legal recognition to digital signatures and fight cyber crimes. The law has been amended in the year 2009 prescribing stringent punishment for cyber crimes such as data theft, piracy, damage to computers and data, pornography and terrorism. The offences have been made cognizable and any police officer of the rank or police inspector or above has been given powers to investigate a cyber crime. The punishment prescribed is harsh including imprisonment of 3 years and also more and fine.

I wish you a safe and secure experience on computer and internet.

SYSTOOLS MAILXAMINER: THE FORENSIC TOOL FOR EMAILS

Mr. Debasish Pramanik*

Why is a forensic tool required for emails?

Emails are a speedy, economical and ubiquitous method of exchanging messages. Today, more than 80% of professional communication occurs through emails. A typical email contains a message that forms the bulk of the communication. The email also contains bits of information that normally are not visible to the user. While emails are an efficient carrier of useful messages, sometimes, they hold clues to dark and sinister scenarios. Analysis of these messages and bits of information can serve as evidence of a wrongful activity.

These threatening scenarios could include:

- Theft of data
- Dishonor of agreements
- Not meeting commitments
- Leakage of confidential information
- Fraud
- Mismanagement
- Victimization
- Harassment
- Coercion
- Cheating
- Deception
- infidelity

To detect threats, you need an easy to use yet powerful tool to ferret slivers of information from voluminous quantities of emails. The tool needs to find patterns of activities and deliberate sequence of tasks from the data. The reports from this tool should serve as legally admissible evidence that helps win disputes in your favor. You need the MailXaminer from SysTools.

* Co-Founder and Product Specialist-Digital Forensics SysTools Software.

Who needs SysTools MailXaminer?

- **Digital Investigators:** These are professionals who examine data in emails and gather evidence of a cyber-crime to be followed by fixing of responsibilities.
- **Law Enforcement Agencies:** These agencies are faced with an increasing number of cases in which emails form the bulk of evidence.
- **Legal Fraternity:** Often, the lawyers formulate their litigation using material culled from emails.
- **Corporate:** With employees communicating inside and outside their enterprise through emails, the management needs clever tools to monitor messages for operational intelligence and evidence of malpractices. This could include forewarning of employees' eminent departure from this job, to harassment, threats and victimization, to data theft and information leakages.
- **Other users:** Investigators of domestic fraud or marital infidelity often find clues and evidence hidden in emails.

What will SysTools MailXaminer deliver?

The MailXaminer delivers clear, unambiguous reports of the conducted search. These searches provide evidence of an event, activity or pattern from within the emails. This foolproof logic behind the gathering of evidence removes all subjectivity and conjecture. This ensures that this evidence can stand the scrutiny of a legal litigation. No longer can suspicions of a wrongful act through email be brushed aside due to lack of scientific proof.

Why SysTools MailXaminer?

- Easy to buy, easy to install, easy to use.
- Low cost of ownership.
- Comprehensive customer support available anytime and anywhere.
- Complex search capabilities using advanced algorithms.
- Easy to operate, even by non-technical users.
- User friendly and logical graphical interface.
- Speedy results, even while searching huge volumes of data.
- Minimal learning curve delivering rapid results.
- Ability to decrypt password protected documents, corrupted or damaged files.
- Sifts through various email variants, even if the client software is not installed on the computer.

- Avoids involvement of external agencies into investigation to ensure secrecy in investigation.
- Reduces dependence on trained manpower and their expensive skills.

ꕥ

The Criminal Law (Amendment) Act, 2013: Legislative Remedies for Online Harassment and Cyberstalking in India

Dr. Sapna Sukrut Deo*

Introduction

The Internet has become a medium for people to communicate globally in the course of business, education and their social lives. The Internet has made it easy for people to communicate, meet a companion, or compete with people on the other side of the world with click of a mouse.

In 2013, according to the *Internet World Stats Report*, 137,000,000 people used Internet, and 56,698,300 people used *Facebook* in India, as a result there arises a concern for Internet safety. The increased use of the Internet has created an impact on the number of online harassing/cyberstalking cases.

Cyberstalking is a new form of computer related crime, occurring in our society. Cyberstalking means when a person is followed and pursued online, invading his/her privacy as his/her every move watched. It is a form of harassment that can disrupt the life of the victim and leave him/her feeling very afraid and threatened. Cyberstalking usually occurs with women, who are stalked or harassed by men, or with children who are stalked by adult predators or pedophiles. Cyberstalkers need not have to leave their home to find, or harass their targets, and has no fear of physical violence since they believe that they cannot be physically touched in cyberspace. They use Internet, e-mail, and other electronic communication devices to stalk persons.

This paper addresses the issue of cyberstalking and online harassment, and what legal remedies an Internet user may have when confronted with this form of behavior. Firstly, the paper will examine what constitutes cyberstalking and harassment, and will discuss the way in which the Internet may facilitate such behavior.

The nature of the behavior is effects-based one upon the victim wherein the stalker is anonymous, although the harasser may not be so. Online harassment is similar to real world stalking in the way that

* Assistant Professor, New Law College, Bharati Vidyapeeth Deemed University, Pune.

it can be disturbing to the victim. At the same time the unique environment of the Internet creates "remoteness" on the part of the stalker, and provides a false sense of security arising from the apparent anonymity that is present on the Internet.

Secondly, this paper will review the current harassment legislation in India, and examine how this legislation has been applied by the Indian courts. In addition it will provide remedies for an Internet user confronted with this behavior.

Finally, the paper will consider "self prevention/protection" measures that individuals may adopt in dealing with online harassment and cyberstalking.

Definitions of Online Harassment and Cyberstalking

Cyberstalking involves using the Internet, cell phone, and/or any other electronic communication device to stalk another person. It may involve threats, identity theft and damage to data or equipment, solicitation of minors for sexual purposes, and any other form of repeated offensive behavior.

Online harassment can involve sexual harassment which is unwanted contact of a personal nature, or other conduct based on sex affecting the dignity of men and women at work.[1] This may include unwelcome physical, verbal or non-verbal conduct. It is unwanted if such conduct is unacceptable, unreasonable and offensive to the recipient. Sexual attention becomes sexual harassment if it is persistent and once rejected by the recipient. However, a single act, if sufficiently serious, can also constitute harassment.[2]

Online harassment can be divided into direct and indirect harassment. "Direct" harassment includes the use of pagers, cell phones and the email to send messages of hate, obscenities and threats, to intimidate a victim. E.g., the majority of offline stalkers will attempt to contact their victim, and most contact is restricted to mail and/or telephone communications. On the other hand "indirect" harassment includes the use of the Internet to display messages of hate, threats or used to spread false rumours about a victim. Messages can be posted on web pages, within chat groups or bulletin boards. This form of harassment is the electronic equivalent of placing pinups on a factory wall, and if the display of such material

[1] http:www.mindspring.com\~techomom\harassed\ (last visited May 1, 2013).
[2] British Telecommunications PLC v. Williams, (1997) IRLR 668.

from the victim's perspective causes offence it will amount to harassment.[3]

Thus generally speaking, online harassment becomes cyberstalking when repeated unwanted communications, whether direct or indirect, takes place over a period of time, via one or more mediums of Internet or electronic communications. The messages themselves must be unwanted, and the content can be-but is not limited to-threatening, sexually harassing, emotionally harassing or bullying, or general misinformation. Provided the messages create reasonable fear in the victim, they fit the definition for cyberstalking.[4]

There are a number of definitions of stalking that exist, each differing slightly. Stalking as "a course of conduct directed at a specific person that involves repeated (two or more occasions) visual or physical proximity, nonconsensual communication, or verbal, written, or implied threats, or a combination thereof, that would cause a reasonable person fear". It is interesting that the definition excludes most electronic forms of stalking as there is often a lack of visual or physical proximity in such cases.[5]

The definition used in the *British Crime Survey*[6] is that stalking is "two or more incidents causing distress, fear or alarm of obscene/threatening unwanted letters or phone calls, waiting or loitering around home or workplace, following or watching, or interfering with, or damaging personal property carried out by any person". In parallel, the psychiatric literature has defined stalking as a course of conduct by which one person repeatedly inflicts on another unwanted intrusions to such an extent that the recipient fears for his or her safety.[7] Whilst each source offers its own interpretation, repetition leading to fear is a recurring theme in any definition.[8]

Stalking and harassment are distinctive in law since the offending behavior is said to occur only when the victim reports him/her self to be distressed as a result of the behavior of another to whom they believe to be threatening. The victim's perception of the offending

---

[3] J. ANGEL, COMPUTER LAW 17 (4th ed. Blackstone Press Ltd, London, U.K. 2000).

[4] Randy McCall, *Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada-Concepts and Recommendations*, www.vaonline.org (last visited May 15, 2013).

[5] Patricia Tjaden & Nancy Thoennes, *Stalking in America: Findings from the National Violence against Women Survey* (1998), http://www.ncjrs.gov/pdffiles/169592.pdf.

[6] K. Smith, K. Coleman, S. Eder & H. Hall, *Homicides, Firearm Offences and Intimate Violence*, 2 CRIME IN ENGLAND AND WALES 1-97 (2009/10.)

[7] *Id.*

[8] http://www.beds.ac.uk/research/irac/nccr (last visited May 6, 2013).

behavior and its effects are therefore pivotal in providing criteria on which to make a charge.

Online Harassment and Cyberstalking in India: Legislative Remedies

Since the 1990s, stalking and harassing has become a common occurrence due to Internet.

In 2001, India's first cyberstalking case was reported. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, *www.mirc.com* using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same.

1. The Information Technology (Amendment) Act, 2008

As a result, **Section 66A** of the Information Technology (Amendment) Act, 2008 (hereinafter the IT Act, 2008) states:

> **Punishment for sending offensive messages through communication service, etc.-** Any person who sends, by means of a computer resource or a communication device,-
> (a) any information that is grossly offensive or has menacing character; or
> (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device;
> (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages
> shall be punishable with imprisonment for a term which may extend to 3 years and with fine.

The IT Act, 2008 does not directly address stalking. But the problem is dealt more as an 'intrusion on to the privacy of individual' than as regular cyber offences which are discussed in the IT Act, 2008. Hence the most used provision for regulating cyberstalking in India is Section 72 of the IT Act, 2008 which runs as follows:

> **Section 72: Breach of confidentiality and privacy.-** Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 Lakh rupees, or with both.
>
> **Section 72A: Punishment for disclosure of information in breach of lawful contract.-** Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to 3 years, or with a fine which may extend to 5 lakh rupees, or with both.

In practice, these provisions can be read with **Section 441 of the Indian Penal Code, 1860** which deals with offences related to criminal trespass and runs as follows:

> Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with an intent to commit an offence, is said to commit criminal trespass.

2. The Criminal Law (Amendment) Act, 2013

Prior to February 2013, there were no laws that directly regulate cyberstalking in India. In 2013, Indian parliament made amendments to the Indian Penal Code, 1860 introducing cyberstalking as a criminal offence.[9]

After 'the December 2012 Delhi gang rape incidence', the Indian government has taken several initiatives to review the existing criminal laws. A special committee under Justice Verma was formed for this purpose and basing upon the report of the committee, several new laws were introduced. In this course, anti-stalking law was also introduced. The Criminal Law (Amendment) Act, 2013 added **Section 354D** in **the Indian Penal Code, 1860** to define and punish the act of stalking. This section is as follows:

(1) Whoever follows a person and contacts, or attempts to contact such person to foster personal interaction repeatedly, despite a clear indication of disinterest by such person, or whoever monitors the use by a person of the Internet, email or any other form of electronic communication, or watches or spies on a person in a manner that results in a fear of violence or serious alarm or distress in the mind of such person, or interferes with the mental peace of such person, commits the offence of stalking:

Provided that the course of conduct will not amount to stalking if the person who pursued it shows-

(i) that it was pursued for the purpose of preventing or detecting crime, and the person accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state; or

(ii) that it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

(iii) that in the particular circumstances the pursuit of the course of conduct was reasonable.

(2) Whoever commits the offence of stalking shall be punished with imprisonment of either description for a term which shall not be less than 1 year but which may extend to 3 years, and shall also be liable to fine.

[9] The Criminal Law (Amendment) Act, No. 13 of 2013, INDIA CODE (2013).

Stalking has been defined as a man who follows or contacts a woman, despite clear indication of disinterest to such contact by the woman, or monitoring of use of Internet or electronic communication of a woman. A man committing the offence of stalking would be liable for imprisonment up to 3 years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to 5 years and with fine.[10]

The term "cyberstalking" can be used interchangeably with online harassment. Cyberstalker does not present a direct threat to a victim, but follows the victim's online activity to collect information and make threats or other forms of verbal intimidation. A potential stalker may not want to confront and threaten a person offline, but may have no problem threatening or harassing a victim through the Internet or other forms of electronic communications.

Enforcement Problems

"Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies."[11]

These problems pertain mainly to international aspects of the Internet. It is a medium that can be accessed by anyone throughout the globe with a computer and modem. This means, as explained below, that a potential offender may not be within the jurisdiction where an offence is committed. Anonymous use of the Internet, though beneficial in many instances, also promises to create challenges for law enforcement authorities.[12]

The Internet is a global medium regardless of frontiers, and this creates new possibilities for the so-called cyberstalker. Cheap and easy access to the Internet means that distance is no obstacle to the cyberstalker.[13] Anyone can become a target for a cyberstalker through the use of the Internet in many forms. The victim can be contacted by e-mail, instant messaging (IM) programs, via chat

---

10 http://en.wikipedia.org/wiki/Criminal_Law_%28Amendment%29_Act,_2013 (last visited May 1, 2013).

11 B. Jensen, *Cyberstalking: Crime, Enforcement and Personal Responsibility in the Online World*, http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm (last visited May 1, 2013).

12 L. Ellison & Y. Akdeniz, *Cyberstalking: The Regulation of Harassment on the Internet*, CRIMINAL LAW REVIEW-*CRIME, CRIMINAL JUSTICE AND THE INTERNET* 7 (Special ed. Dec. 1998).

13 *Id.*

rooms, social network sites, or the stalker attempting to take over the victim's computer by monitoring what he is doing while online. The Internet is not a "lawless place"[14], and there are difficulties in applying laws that are made for specific nation states and this would be also true of applying national harassment and stalking laws to the Internet.

Self-help Approaches

After researching on various aspects of cyber talking, the problem came to know is that the limitations of legal regulation of online harassment in cases which involve anonymous cyberstalkers. These limitations in legal regulation are, to some extent, compensated for by the availability of non-legal solutions to online harassment. A number of more suitable ways in which users can protect themselves from online harassment are discussed below.

- Do not share personal information in public spaces anywhere online, nor give it to strangers, including e-mail or chat rooms.
- Do not ever reply to offensive, defamatory, provocative e-mails if you get them.
- Do not respond to flaming, or get provoked online.
- You can use online segregating tools such as blocking of the email ID, reporting of spams, and are also advised to use strong encryption programmes such as the Pretty Good Privacy (PGP) which ensure complete private communications.
- If you are being stalked, you don't have to be a victim. Report the incident to your Internet Service Provider, police station in your city, or an online help agency and also take advice from your techno-savvy friends.
- Keep evidence of possible harassment by saving messages, or copying and pasting them to self e-mails. Prevention is always better than cure.

[14] *See* J.R. Reidenberg, *Governing Networks and Cyberspace Rule-Making*, 45 EMORY LAW JOURNAL 911 (1996).

PROBLEMS AND SOLUTIONS FOR CYBER CRIMES

Mr. Vaibhav Salunkhe*
Mr. Balkrishna Jadhav†

1. Credit Card Fraud

Problem:

Tushar is assistant manager with the fraud control unit of a large business process outsourcing (BPO) organization. The BPO facility has about 350 employees. Their primary function is to issue the bank's credit cards as well as attend to customer and merchant queries. Each employee is assigned to a specific task and is only allowed to access the computer system for that specific task. The employees are not allowed to make any changes in the credit card holder's account unless they received specific approvals.

Each of the employees is given a unique individual password. In case they entered an incorrect password three consecutive times then their password would get blocked and they would be issued a temporary password.

The company suspected that its employees conspired with the son (holding an add-on card) of one of the credit card holders. The BPO employee deliberately keyed in the wrong password three consecutive times (so that his password would get blocked) and obtained a temporary password to access the computer system. He manually reversed the transactions of the card so that it appeared that payment for the transaction has taken place. That person also changed the credit card holder's address so that the statement of account would never be delivered to the primary card holder.

Solution:

- Tushar can lodge a complaint by going to the nearest police station.
- Section 66-C of the Information Technology Act, 2000 provides punishment for identity theft. According to this Act the person can be punished with imprisonment upto 3 years and fine upto Rs.1 lakh.

* Practicing Cyber Lawyer, Pune.
† Independent IT Security Consultant, Pune.

- It is also punishable under Section 420 of the Indian Penal Code, 1860.
- Police can visit the premises of the BPO and conduct detailed examination of various persons to understand the computer system used.
- Police can analyze the attendance register which showed that who was present at all the times when the fraudulent entries had been entered in the system. They also analyze the system logs that showed that the accuser's ID had been used to make the changes in the system and corresponding CCTV Coverage .
- Police can trace IP address to service provider and ultimately to the person who is involved in the crime.

2. Online Railway Ticket Fraud

Problem:

Ram is an online railway ticket booking service provider. one day he found that some unknown people had used the internet ticket booking facility to book 44 railway tickets using stolen credit card details.

Due to this incident Ram has to bear lots of finacial losses. Ram understood that he is being cheated. Now he wants to recover his money.

Solution:

- Ram can lodge a complaint by going to the nearest police station.
- Section 66-C of the Information Technology Act, 2000 provides punishment for identity theft. According to this Act the person can be punished with imprisonment upto 3 years and fine upto Rs.1 lakh.
- It is also punishable under Section 420 of the Indian Penal Code, 1860.
- The department will receive chargeback from the credit card companies for all the 44 transactions causing huge financial losses.
- Police will investigate all user IDs created by accounts as well as IPs involved in the fraud.
- Police will recover all user accounts and their passwords.
- Police will also investigate stolen credit cards of various accounts.

3. Lottery Scam

Problem:

Govind is government employee. He likes to surf internet. He also loves to register many sites available on net to get updates.

One day Govind got an *e*-mail from U.K. NATIONAL LOTTERY. It was mentioned in the lottery that Govind has won Rs.50 lakhs. So he contacted those people and verified the details.

Those people demanded Govind Rs.5 lakhs as security deposit and other charges and told him that he will regain his Rs.5 lakhs with Rs.50 lakhs. After verification Govind sent Rs.5 lakhs amount to get his Rs.50 lakhs; but after paying the money, those lottery people stopped contacting Govind. He tried to contact them but numbers were not in service at that time.

Govind is now feeling that he is being deceived and he wants his money back.

Solution:

- Govind can lodge a complaint by going to the nearest police station.
- Section 66-C of the Information Technology Act, 2000 provides punishment for identity theft. According to this Act the person can be punished with imprisonment upto 3 years and fine upto Rs.1 lakh.
- It is also punishable under Section 419 of the Nigerian Fraud Legislation on "advanced fee fraud", Section 66-D of the Information Technology Act, 2000, Section 420 of the Indian Penal Code, 1860.
- Police will also investigate the bank accounts used in the fraud.
- Police will investigate the IPs of the sender of the *e*-mail as well as phone numbers used in the scam.

4. Fake Travel Agent

Problem:

Neehar was posing as a genuine railway ticket agent and had been purchasing tickets online by using stolen credit cards of non-residents. Neehar created fraudulent electronic records/profiles, which he used to carry out the transactions.

The tickets so purchased were sold for cash to other passengers. Such events occurred for a period of about 4 months.

The online ticket booking service provider took notice of this and now wants to find the fraudster.

Solution:

- The online ticket booking service provider can lodge a complaint with the Cyber Crime Investigation Cell.
- Section 66-D of the Information Technology Act, 2000 provides for the punishment for cheating by impersonation. According to this Act the person can be punished with imprisonment upto 3 years and fine upto Rs.1 lakh.
- Police can trace IP address to service provider and ultimately to the person who is involved in the crime.

5. Illegal Money Transfer

Problem:

Rohit was working in a BPO that was handling the business of a multinational bank. Due to nature of his work and project he regularly had access to sensitive database of the customers of bank.

Rohit, during the course of his work obtained personal identification numbers (PIN) and other confidential information of the bank's customers.

Rohit and his accomplices, using this information transferred huge sums of money from the accounts of different customers to fake accounts through different cyber cafes. Total INR 19 million was transferred.

Solution:

- Neeta can lodge a complaint by going to the nearest police station.
- Section 66-C of the Information Technology Act, 2000 provides punishment for identity theft. According to this Act the person can be punished with imprisonment upto 3 years and fine upto Rs.1 lakh.
- It is also punishable under Section 420 of Indian Penal Code, 1860.
- Police can lay a trap in a local bank where they had fake accounts for illegally transferring money. IP addresses can be traced to the

internet service provider and ultimately to the cyber cafes through which illegal transfers were made.
- Police can freeze the fraud accounts.

6. Online Stock Exchange Fraud

Problem:

Pritesh is working in a company, which does dealing in sale and purchase of shares on behalf of clients. As a broker of the stock exchange they were providing trading facilities of the equity and futures and options markets to their sub-brokers/high net worth individual clients. They do this at the clients' premises through ISDN lines/normal telephone lines/VPN with predefined passwords and user IDs on their trading terminals.

A fraudulent trade was executed by selling a call option by using the user ID and password provided to one of Pritesh's client. An interesting aspect was that this call option was most inactive for trading purposes and no trade had taken place except for the fraudulent trade.

The said call option was compulsorily exercised by the exchange thus resulting in a loss of INR 0.05 million to Pritesh and wrongful gain to the fraudster.

Solution:

- Pritesh can lodge a complaint by going to the nearest police station.
- Section 66-C of the Information Technology Act, 2000 provides punishment for identity theft. According to this Act the person can be punished with imprisonment upto 3 years and fine upto Rs.1 lakh.
- It is also punishable under Section 420 of Indian Penal Code.
- Police will ask for information to company for the following:
  Date - Buy Client Name/Address
  Trade Number - Sell Member Code
  Trade Time - Sell Trading Member Name
  Trade Quantity - Sell Client Code/Name/Address
  Buy Time - Buy Order Number
  Buy Name - Sell Order Number
  Buy Client Code

Police will investigate IPs, firewall logs of company, server logs, *e*-mail IDs, computer systems of company.

PROTECT YOURSELF: CYBER CRIMES SECURITY TIPS*

1. Mobile Theft

- Contact your telecoms service providers: they can block your SIM card and thereby prevent any fraudulent use.
- You will be asked for your mobile number, proof of ID and IMEI code which is given in purchase receipt of your mobile handset.
- File a police report as soon as possible, including a description of your handset, and the serial and/or IMEI code.
- Police can track the location of mobile phone by tracking its IMEI number.

Legal Remedies:

- Section 379 of the Indian Penal Code, 1860 upto 3 years imprisonment or fine or both.
- Section 66 B of ITAA, 2008–upto 3 years of imprisonment or Rs.1 lakh fine or both.

Security Tips:

- Set a complex password that you'll remember but thieves won't guess (don't use common passcodes like 1234 or 0000).
- Set your screen to auto-lock within five minutes.
- Smartphones incorporate GPS functionality, which when enable can help to track the mobile.
- Make habit to take regular backup of your mobile data. Many service providers offer this service free of charge.
- Download a mobile security app such as *Lookout* is an extra layer of protection for your mobile.

2. Sending Unwanted Messages/Calls

- Lodge a complaint by going to the nearest police station against all the mobile numbers which sends unwanted sms or gives unwanted call.
- Police can investigate the complaint under Information Technology Act, 2000, Indian Penal Code, 1860 and Telephone Regulatory Act of India, 1997.

---

*Dr.Sapna Sukrut Deo, Assistant Professor, New Law College, Bharati Vidyapeeth Deemed University, Pune.

- At first police will contact with the service provider from whose number the calls and multiple sms are coming and will acquire the identification of the users and will file cases against them.
- If the identification of the users cannot be made by the service providers then the service provider can stop the services of those numbers under Telephone Regulatory Act of India, 1997.
- There is no need to change the number.

Security Tips:

- You can opt for the call barring facilities from your phone and blacklist the numbers in your phone. Look out for in-built or downloadable option to limit incoming calls.
- You can avail your service provider to activate DND services on your phone if phones are from telecallers or marketing companies.

3. Indentify Theft

- Criminals gets your identity from social networking websites, job sites, matrimonial sites, special offers discounts coupons by registrations, stolen wallets, online shopping , many more. If you suspect that someone has used your identity immediately lodge a complaint by going to the nearest police station.
- Police can investigate the complaint under Section 66(C)) for Identity theft and if your identity theft is used for sending offensive messages then under Section 66(A) of the Information Technology (Amendment) Act, 2008 (ITAA, 2008).

Legal Remedies:

- Section 66(C) of ITAA, 2008–upto 3 years of imprisonment or fine upto Rs.5 lakhs or both.
- Section 66(D) of ITAA, 2008–upto 3 years imprisonment and fine upto Rs.1 lakh.

Security Tips:

- Make your password long, strong and unique, with a mix of upper and lowercase letters, numbers and symbols.
- Do not share your personal data details over phone or by mail or on social networking sites.
- Only accept friend requests from those you know on social networking sites.

- Don't use the same user name and/or passwords on social media sites that you do on your credit card or bank sites.
- Do not save personal files in a cyber café's or friends PC.
- Remove matrimonial profiles from sites, once the purpose is achieved.
- Do not use the same email id to received financial information or transactions.

4. Fake Profile on Matrimonial Websites

- Posting incorrect information on age, religion or marital status are the most common problems in online marriage portals, as is lying about salary. If you are a victim of fake or misrepresented matrimonial profiles on online portals. You can directly file a complaint before the Adjudicating Officer, Ministry of Information Technology, Information Technology Act, 2000.
- The format for the complaint can be obtained from the website and is required to be on a plain paper and submitted along with the fees payable, which is calculated on the basis of damages claimed by way of compensation.
- The police can traced real face behind the fake profile through the IP address or bank account details used to make paid profiles online.
- This is punishable under Section 66(C) of the Information Technology Act, 2000 which provides punishment for identity theft.
- The online dating and matrimonial portals being "intermediaries" can be held liable under Section 79(3)(a) of the Information Technology Act, 2000 if: "The intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act".

Security Tips:

- It is better to check credentials of the matrimonial site before registering .
- For choosing life partner first it is important to find out that whether that matrimonial site is registered or not.
- Check the authenticity of that website by asking people or friends.
- To create a good profile sometimes wrong qualification or job description is given. Verify the qualifications with certificates.
- Check the job description by verification on the job site or in the company and by speaking with the company authorities.

- If the person is NRI or foreign resident proper enquiry is company from his work place.

5. Phishing Scam

- The phishing fraud is an online fraud in which the fraudster disguise themselves and use false and fraudulent websites of bank and other financial institutions, if you think you are a victim of phishing Lodge a complaint by going to the nearest police station.
- Police can set up a trap in a local bank for investigating fake accounts.
- If fraudulent money is transferred online then police can trace IP address to service provider and ultimately to the person who is involved in illegal money transfer.

Legal Remedies:

- The account of the victim is compromised by the phisher which is not possible unless and until the fraudster fraudulently effects some changes by way of deletion or alteration of data electronically in the account of the victim residing in the bank server. Thus, it is punishable under Section 66 of the Information Technology Act, 2000.
- The disguised email containing the fake link of the bank is used to deceive or to mislead the recipient about the origin of such email and thus, it is punishable under Section 66(A) Information Technology Act, 2000.
- In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say logo, trademark etc., and thus, it is punishable under Section 66(C) of the Information Technology Act, 2000.

Security Tips:

- Banks never asks your passwords or PIN number by mail. Never respond to these questions.
- Do not click on hyperlinks or links attached in the email that asks you to provide confidential data.
- One should install security measures that will block the phishing mails as well as phishing sites.
- Check the email if it is addressed in your name. Your bank will always refer you with your name while fraudsters will refer you as “Dear Customer” or “Dear Valued Customer”

because they send emails randomly to a million email addresses.

- Never enter your credit card details and password in a website.
- Do not share your account details, password, or credit card details with anyone who you do not know or trust.
- Log in to your accounts regularly and look for account transactions that you do not recognize.

6. Capturing, Publishing, or Transmitting Picture of a Private Area without Person's Consent or Knowledge

- Lodge a complaint by going to the nearest police station.
- Police can lodge complaint under Section 66(E) of the ITAA, 2008 for punishment for violation of privacy which is upto 3 years imprisonment or fine not exceeding Rs.2 lakhs or with both.

Security Tips:

- Beware of hidden cameras in trial rooms, bathrooms, hotel rooms, changing rooms, toilets, etc.
- In front of the trial room take your mobile and make sure that mobile can make calls. If u can't make a call; you can check that may be there is a hidden camera. This is due to the interference of fiber optic cable during the signal transfer.

7. Hate Speech

- Any individual, who through the medium of social media writes content as form of a "comment" which incites communal hatred and/or violence, will be held accountable under Section 153A of the Indian Penal Code, 1860.
- The punishment stipulated under this section is 3 years' imprisonment with a fine.
- Social media should remove such content from its servers once it is brought to its notice. If it fails to remove the content within the 36 hours stipulated by the Information Technology Act Guidelines, it will lose the protection offered under Section 79.
- In such a situation that social media company may be held responsible as a contributing party and its executives may be charged under Section 153A of the Indian Penal Code, 1860.