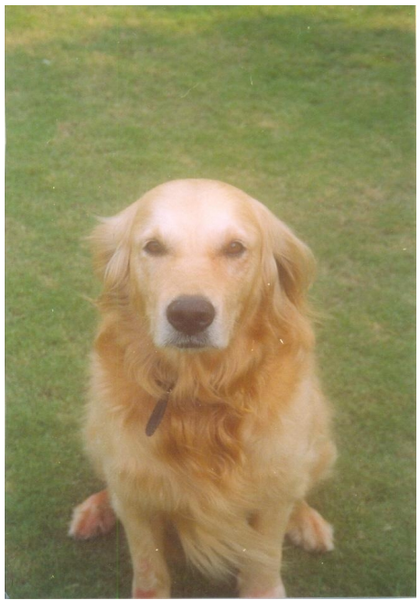
ON THE INTERNET,
NOBODY KNOWS THAT YOU ARE A DOG:
Fundamentals of Cyber crime

(Text of talk delivered by Justice Yatindra Singh, Judge, Allahabd High Court, in cyber meet/ seminar of the IT secretaries and police officials held at Dehradun on 21.5.2011)



Does it matter that on the internet one can be anonymous. Is it a correct statement?Is it relevant for the session on cyber crimes?

Just bear with me for sometime: it is relevant. But first, let's consider as to why cyber law is necessary.

NEED FOR CYBER LAW

Towards the end of the nineteenth century, mathematicians started having doubts about the foundations of their subject. They started searching rigorous proofs of their fundamentals. One area of search was related to the paradoxes around self-referencing. The most famous of all such paradoxes is Epimenides' or liar's paradox? Epimenides (ऍपीमेनेडीज़) was the 6th century Greek philosopher. He was a Cretan. He made an immortal statement:

‘All Cretans are liars’.

It is like, my saying,

'All Indians are liars'

Try analysing it: if you accept it as true, it boomerangs that it is false; If you take it to be false, it backfires that it is true.

A century ago, the Epimenides paradox was reformulated by Bertrand Russell as 'Barber's or Russell's paradox':

'The only barber in the village declared that he shaves only those who do not shave themselves'.

There was no problem with it, till the question is asked,

‘who shaves the barber?’

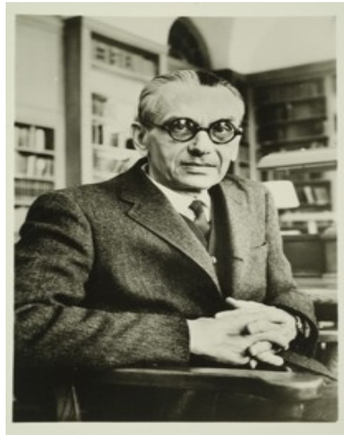
Russell and Whitehead tried to sort it out in ‘Principia Mathmatica’ a giant opus published in 1913. They thought that they had sorted it out but alas, they did not.

Kurt Gödel wrote a paper in 1931. It was in German and its English

translation was titled 'On formally Undecidable Proposition of Principia Mathematica and Related Systems'. Gödel solved such paradoxes forever. He proved that it cannot be solved: The basic idea of the paper was,

> 'Proof of arithmetic consistency is not possible—every system is incomplete.'

This has wide implications and one of them is that there is no fort that cannot be breached; and there is no computer that cannot be hacked—every system, every computer can be hacked.



Kurt Gödel – picture courtesy Institute of Advanced Studies, Princeton

In substance, irrespective of the security measures, there will always be room for improvement. And Security measures will never be sufficient: they have to be backed up with adequate legal sanctions. This is the reason that cyber laws are necessary.

But what is cyber law? Are all violations of cyber law called cyber crimes? Let's take a look at what is cyber law.

CYBER LAWS

Inventions, discoveries, and new technologies widen the scientific horizon but pose new challenges for the legal world. The information technology (brought about by computers, Internet and cyberspace) has opened new dimensions but has also created problems in all aspects of law. We are finding solutions for them. These solutions—statutory or otherwise—providing answers to the problems are loosely referred to as ‘Computer Laws’ or ‘Information Technology Laws’ or simply ‘cyber Laws’.

We have enacted a few statutory provisions. The problems (due to the information technology) in the field of Intellectual Property Rights (IPRs), have been sorted out by amending the Copyright and the Patents Act. However, the most important legislative measure is the Information Technology Act, 2000 (the Act). It has also amended the following four Acts.

(i) The Indian Penal Code, 1860;

(ii) The Indian Evidence Act, 1872;

(iii) The Bankers' Book Evidence Act, 1891;

(iv) The Reserve Bank of India Act, 1934.

Communication Convergence Bill

Another Act, entitled Communication Convergence Bill 2001[1] was in the pipeline. It was to fully harness the benefits of the three converging technologies of the future namely—the Telecom, Information Technology, and Broadcasting.

A committee was set up to consider the Communication Convergence Bill. It recorded sharply divided opinion of the experts about the desirability of having such enactment. This may be the reason that the Bill is still in the cold storage. It may not be enacted in the near future. However, some of its provisions have been incorporated in the Act by an amendment.

Amendments in the Act

An expert committee was set up to consider the amendments in the Act. It has made its recommendations and proposed amendments. The amendments were proposed in 2005. They were introduced in modified form as the Information Technology (Amendment) Bill 2006. The 2006 Bill was further modified and passed by the Parliament on 23.12.2008. After the assent of the President, it was notified on 5.2.2009 as the Information Technology (Amendment) Act 2008 (Central Act no. 10 of 2009)[2] (the 2008 Amendment Act). It has been enforced from 27.10.2009. It has incorporated some important provisions of the Communication Convergence Bill.

Previously mentioned four Acts were amended by Section 91 to 94 of the Act. These sections have been omitted by the amending Act but in view of Section 6A of the General Clause Act[3] these amendments in the respective Acts will continue. The first two Acts have been further amended by the amending Act.

---

1 The complete text of the report of the committee of the Parliament is available is http://164.100.24.208/ls/committeeR/Communication/39.pdf

2 The amendments may seen at: http://www.mit.gov.in/download/it_amendment_act2008.pdf

3 Section 6A of the General Clause is entitled 'Repeal of Act making textual amendment in Act or Regulation'. It states that in such a situation unless different intention appears, the repeal does not effect the continuance of any amendment made by the enactment so repealed. In view of this, the amendments in the aforesaid Acts will continue. Notes on the clauses along with the 2006 Bill also state that sections 91-94 are being omitted for the reason that these provisions have become redundant as necessary modifications have already been carried out in the enactments.

With this in background, let's consider violations of cyber laws and cyber crimes.

CYBER CRIME

Broadly, violations of cyber laws can be divided into two categories:

(a) Violation—Intellectual Property Right (IPR): This can be categorised as:

(i) IPRs problems in the cyberspace. This includes Copyright and Trademark infringement on the Internet, Domain name dispute, Cyber Squatting, Framing, Metatag and key word disputes. peer to peer file sharing etc.

(ii) Illegal copying and distribution of computer software;

(iii) Problems relating to Trade secret, Reverse engineering (Decompilation), and Patents in the computer software.

(b) Violation Other than IPR. This is dealt under the Act and is generally referred to as cyber crime. They can be divided into two categories.

(i) Crime where the computer or server is the object/ target. It includes hacking a computer or a website or a server, sending a virus, Denial of Service (DoS) attack, Adware and Spyware, Data protection, etc.

(ii) Crimes other than those where computer or server is the object/ target but computer is used as an instrument for committing the offence. It includes for example credit card fraud, Phishing, Pornography, identity, theft, violation of privacy, spam, spim, Cyber stalking, Cyber bullying, Cyber terrorism etc.

This distinction of cyber crime is not distinctive and the line between the two is often blurred. One act may fall in both of them. There can also be other criteria for categorising them.

CYBER CRIMES - REMEDIES

Civil as well as criminal proceeding can be taken to remedy the cyber crimes.

Chapters IX and X of the Act deal with the civil remedies:

- Section 43 of the Act (Chapter IX) imposes 'penalties and compensation for damage to computer system etc.
- Section 43A provides compensation for failure to protect data.

These disputes and determination of compensation are not dealt by the civil courts but are entrusted to adjudicating officers having experience in the field of Information Technology. Appeal lies against their decisions to an Appellate Tribunal and then to the High Court;

The offences (criminal proceeding) are dealt with in Chapter XI of the Act. The specific offences (for details see Appendix-1) are punishable under the following sections of the Act:

- Virus, DoS, Adware spyware – section 66 read with 43;
- Cyber stalking, Cyber bullying, Spin, Spam, Identity theft, Violation of privacy, Cyber terrorism - sections 66 A to 66F;
- Publishing and transmitting obscene, sexually explicit material - sections 67, 67A and 67 B;
- Disclosure of information in breach of lawful contract -r section 72A

The Investigation of the criminal case is to be done under Criminal Procedure Code (with some modifications) and cases are to dealt by the criminal courts.

TACKLING—CYBER CRIME

Awareness And Precaution

The best strategy for any crime, be it cyber crime or other, is prevention. The obvious measure is to improve security measures, enhance public education and vigilance. Most of the cyber crimes can be prevented by not answering the emails or at least verifying them and not opening the attachment unless it is from trustworthy person.

Efficient Enforcement—Improving Confidence

Not all cyber crimes—that are in the society—are reported. This is not only true in the case of individuals but also in the case of the corporations. This could be because of lack of the confidence in the people. Quick and satisfactory resolution of the cyber law crime will boost the public confidence. This will bring forward more people with their problems.

PARADOX—INTERNET CYBERSPACE

The title of the article is punch line of the cartoon published by Peter Steiner on 15th July 1993 in the New Yorker: a milestone in many ways.

The cartoon shows two dogs with a computer. The dog sitting in front of the computer keyboard is telling the other,

'On the Internet, nobody knows that you are a dog.'

Cartoon courtesy - Wikipedia

This is the paradox of Internet: the paradox of the cyberspace. This is also the genesis of contraventions in cyberspace. People are emboldened to commit it because they mistakenly assume that they are anonymous but this is not correct.

Well, the truth is, on the Internet, everybody knows that you are a dog. There is nothing private in the cyber space: it is the end of privacy.

CONCLUSIONS

We must guard ourselves against cyber crimes lest it may lead to banking/ trade online catastrophe or compromise in national security. I am glad that this cyber meet has been organised to bring awareness about cyber laws and cyber crimes. It is a step in the right direction.

Appendix-1

(Some common cyber crimes and their punishments are mentioned below. Mobiles phones are getting smarter. Smart-phones have almost all functions of a computer. The following offences may be committed with the help of a computer or a mobile phone or any other communication device.)

Cyber Crimes

Tampering Source Code: Tampering with the computer source document is punishable under Section 65 of the Act,

Virus attack/ Malware: Virus attack/ Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It includes viruses, worms, Trojans, rootkits, backdoors, spyware, botnets, keystroke loggers and dialers. It is punishable under section 66 of the Act.

Denial of Service (DoS): DoS attack means, preventing legitimate users of a service from using that service. It generally occurs when a web server is flooded with requests for information, overwhelming the system. Although such attacks do not normally compromise information security, they do cost time and money.

It may happen due to—

- flooding a network; or
- disrupting connections between the machines; or
- disrupting service to a specific system or person; or
- preventing a particular individual from accessing a service.
- Illegitimate use of resources.

It is now punishable under section 66 read with section 43 of the Act.

Data Theft: Sensitive information belonging to business organisations is targeted by rivals, criminals and sometimes even by disgruntled employees. Such data (e.g. business plans, tender quotations, etc) may be obtained using hacking or social engineering techniques. It is punishable under sections 66 & 66B of the Act.

Spyware and Adware: These two words are often used together and there is a thin line of difference between the two. They are often referred to

the programmes that get installed on your computer without or with your permission (perhaps granted unwittingly).

- Spyware installs itself surreptitiously and is difficult to remove without assistance;
- Adware generally comes with an uninstaller, and can be easily removed from a system.

These programmes can drain your computer's resources, slow your Internet connection, spy on your surfing, and even forcibly redirect your Web browser. They are now punishable under section 66 read with 43 of the Act.

Cyber Espionage and Cyber Spying: Cyber espionage or cyber spying is the act of obtaining personal, sensitive, proprietary or classified information without permission. It involves the use of cracking techniques and malicious software including Trojans and spyware. It is punishable under section 66 of the Act.

Cyber Stalking and Cyber Bullying: Stalking, is the crime of following and watching somebody over a long period in a way that is annoying or frightening. It generally involves, harassing or threatening behaviour that an individual engages repeatedly such as, following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. The term cyber stalking, broadly refers to the use of the Internet, email, or other electronic communication devices, to stalk another person.

Cyber bullying is bullying a person in the cyber space.

Spam and Spim: Spam is an unsolicited mail. Spim is the chat clients what spam is to email. It is junk or unsolicited instant message (IM).

Phishing: Phishing is a fraudulent way of getting confidential information. In phishing, unsuspecting users receive official-looking emails that attempt to fool them into disclosing online passwords, user names and other

personal information. Victims are usually persuaded to click on a link that directs them to a doctored version of an organization’s Website.

Cyber Stalking, Cyber bullying, Spam, Spim, and **Phishing** are now punishable under section 66A of the Act.

Identify Theft: Identity theft involves the fraudulent or dishonest use of someone's electronic signature, password or other unique identification feature. It is punishable under section 66C of the Act.

Violation of Privacy: Publishing or transmitting pictures of a private area of a person without consent is violation of privacy. It is punishable under section 66E of the Act.

Cyber Terrorism: Cyber terrorism involves the use or threat of disruptive cyber activities for ideological, religious or political objectives. It can weaken a country's economy and even make it more vulnerable to military attack. It is punishable under section 66F of the Act.

Financial Crimes/ Cyber Frauds: This is a wide term that includes credit card fraud, online share trading scams and e-banking crimes. It is punishable under sections 66 and 66D of the Act.

Punishments

Section 65: Imprisonment upto 3 years or a fine upto rupees 2 lakhs or both.

Section 66: Imprisonment upto 3 years and fine upto rupees five lakhs or both.

Section 66A: Imprisonment upto 3 years and fine.

Section 66B to 66 D: Imprisonment upto 3 years and fine upto rupees one lakh.

Section 66E: Imprisonment upto three years or fine upto two lakhs or both.

Section 66F: Upto imprisonment for life.

Section 67: Imprisonment upto five years and fine up to ten lakhs rupees.

Section 67B: Imprisonment upto five years and fine upto ten lakh rupees for the first conviction. And on the subsequent conviction imprisonment upto seven years and fine upto ten lakh rupees.

Section 72A: Imprisonment upto three years or fine up to five lakhs rupees or with both.