LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

Legal Provisions with reference to Hacking: a Global Scenario*

INTRODUCTION

Hacking refers to activities aimed at attempting or gaining unauthorized access to IT systems. Controversies still exist over its definition since some experts believe that hacking is both ethical and unethical. Hackers of the earlier era shared certain ethics and believed in unrestricted access to technology and freedom of information. In a way, major developments in the fields of personal computers and software technology can be attributed to hackers. With passage of time, ethics shattered and by 1980s the malicious hacker was born whose *modus operandi* involved breaking into computers and/or networks to steal proprietary information with intended misuse.

The Internet has paved way to commit crimes anywhere around the globe without physically entering the jurisdiction where the crime is committed. Thus, apprehending and trying cyber criminals becomes very challenging. Further, the ways and means of hacking are fast evolving. Nonetheless, in order to protect the confidentiality, integrity, and access to data and systems from unauthorized intrusion, efforts must be made to make appropriate legislation in order to combat the problem of cyber crimes.

The provisions affecting the Confidentiality, Integrity and Availability of data will be studied under three heads i.e. Council of Europe Convention on Cyber Crime 2001, The Information Technology Act, 2000 and the US Law (Federal Law provisions).

Evolution of Cyber Space, Cyber crime and Hacking.

Cyber Space the term as understood today means the virtual world created by mankind using computers and networking through which one interacts and exchange information using multiple languages or communication protocols that are created by humans so that one computer can talk to another computer.[1] However the term seems to find its origin in the short story 'Burning Chrome" of William Gibson which was published in Omni Magazine. The story was about hacker group "Cyberspace Seven" where it was visualised as to how individuals shift their consciousness from the physical world into virtual world. The linkage between cyberspace and crime was yet another step which gave rise to the term Cybercrime. William Gibson in his stories has defined ***cybercrime*** as harmful activity that takes place in virtual environments which made

* **Mrs. Vaishnavee Sagar Pawar, Dr. Santosh A. Shah, Dr. R.K. Kamat, Shivaji University, Kolhapur – 416 004.**

[1] KARNIKA SETH, COMPUTERS, INTERNET AND NEW TECHNOLOGY LAWS, 8 (1st ed. Lexis Nexis Butterworths Wadhwa 2012)

the hi-tech hacker a norm in the entertainment industry.[2] This is evident from the Hollywood movies which portrayed the fusion of cyberspace and crime whether it may be war games (1983) portraying computer hacking as a danger to national security or The Net (1995) where it is shown as to how technology is used to commit crimes like Identity Theft or Die Hard 4.0 where state hits back with the help of an ethical hacker.

Technological development in the field of personal computer and networking is no doubt a boon to society but also paved way to commit new forms of cybercrimes. The architecture of Internet being decentralized has created opportunities for cybercriminals to commit transnational crimes. So, cybercrimes can be described as crimes that are committed by using networked technologies. The term has assumed a global dimension and is becoming a part of legal terminology which can be seen in the form of Council of Europe Convention on Cybercrime.

History of Hacking

The origin of the term Hacking can be traced to MIT where model train was hacked out of curiosity to see how things worked. The first generation computers were massive machines which were expensive and access to these computers was restricted to limited number of people. The hackers of the then era were curious of knowing as to how computers worked, they believed in unrestricted access of computers and were of view that information should be free. The hackers believed in open source movement, software to be developed and distributed so that it can be improvised by anyone.

Some of the well known hackers of the then era are Bill Gates and Paul Allen, founders of Microsoft. But with the passage of time very few adhered to hacker culture one of them was Richard Stallman. Companies started to be formed where the pure approach regarding open source was lost and information started to become proprietary as we can see Windows and Apple.

A new creed of hackers is born who are no more interested in exploring things but they will use their technological knowledge and skill to break into computers and network to steal confidential information. This led categorization of hackers by different names depending upon the intrusions they committed.

Hacker: Hacker is a person who intends to gain unauthorized access but does not indulge in unauthorized penetration of computer systems (break-in) or viewing others' files without permission rather having technical capabilities. A computer technology expert who "does the impossible" proves his or her ability and superior expertise and belongs to an elite subculture of experts in the field who are leading society towards a better technological future.[3]

Cracker: Cracker is a person with criminal intent. According to the Jargon Dictionary, the term began to appear in 1985 as a way to distinguish between hacker and cracker. A cracker is a person who maliciously sabotages computers, steals information located on secured computers and cause disruption to the networks for personal or political motives.[4]

The tendency to commit cyber crime can be best illustrated by Space Transition Theory according to which people behave differently when they move from one space to another i.e. from physical world to cyberspace. Identity flexibility, anonymity and lack of deterrence are contributing factors which provide means to commit cyber crime.[5]

Council of Europe Convention on Cyber Crime

[2] YVONNE JEWKES, MAJID YAR, HANDBOOK OF INTERNET CRIME, 5 (1st ed. Willan Publishing 2010)
[3] K.JAISHANKAR, CYBER CRIMINOLOGY, 38 (1st ed. CRC Press 2011)
[4] YOGESH BARUA, DENZYL P.DAYAl, *Emergence of Cyber Crime In:* CRIMINAL ACTIVITIES IN CYBER WORLD, 8 (1st ed. Dominant Publishers and Distributors Pvt. Ltd. 2011)
[5] K.JAISHANKAR, CYBER CRIMINOLOGY, xxviii (1st ed. CRC Press 2011)

The Council of Europe Convention was opened for signature on 23rd November, 2001 in Budapest. It is an important International Legislation dealing with matters of cyber crimes and binds nations of the world in the same way as Treaty. The framework of this convention can be divided in four parts:-

1. It provides for a common cross-border criminal policy which aims at protection of society against cybercrimes thereby encouraging nations to adopt appropriate legislation so as to combat the problem of cyber crime.
2. The procedural requirements such as preservation of data, real time collection of traffic data and interception of data to which nation must adhere to in order to overcome the challenges faced by law enforcement officials while collecting evidence due to its volatile nature and as the data can be altered or deleted.
3. It provides guidelines for initiating international cooperation as regards joint investigations in matters of criminal offences which have been provided in Articles.
4. The framework of convention is distributed among 48 Articles. However, categorization of criminal offences has been made in four parts:-

   Part I - *Article 2 to 6* deal with acts affecting Confidentiality, Integrity and Availability of computer systems and data.

The convention is open to all the nations of the world.

In order to avoid over criminalization for minor acts of misconduct, the convention provides that offences under the article should be committed intentionally.

Article 2 to 6 of the convention provides for criminal offences as against the Confidentiality, Integrity and Availability of computer systems or data.

Article 2 – Illegal Access

Acts involving access to computer system without right for instance unauthorized intrusions such as hacking, cracking or computer trespassing.

Article 3 – Illegal Interception

The provision aims to protect right to privacy of data communication by restricting the interception of non-public transmission of computer data. However the use of cookies to track an individual's surfing habits are not criminalized because they are considered to be within rights.

Article 4 – Data Interference

The Article criminalizes infliction of intentional damage that is caused by installation of malicious codes (i.e. virus, worms etc.) resulting in destruction of data and programs within a computer.

Article 5 – System Interference

The Article aims to prevent intentional hindrance caused in the way of lawful use of computer system for instance denial of service attacks which prevent the legitimate user from accessing computer or installation of malicious software which slow down the operation of

system. Spam involving acts of computer sabotage would also be covered under the provisions of this Article.

Article 6 – Misuse of Devices

The Article deals with use of certain devices for commission of illegal acts which are mentioned in *Article 2 to 5*. The Article prohibits sale or trade of hacker tools that facilitate commission of cybercrimes. It covers not only tangible transfers but also creation of hyperlinks that facilitates the hacker to access the devices.

US Legislation on Unauthorized access

Before 1984 there were no specific laws in US prohibiting computer and network crimes including hacking, malicious code and denial of service attacks. Wire and mail fraud Statutes existed but suffered from certain limitations and were not capable of dealing with evolving cyber crimes. A need was felt to enact new laws and so Comprehensive Crime Control Act 1984 was enacted to include unauthorized access and use of computer networks to commit crimes. But later on in 1986 Computer Fraud and Abuse Act (CFAA) was passed, which amended 18 USC _1030. The Statute provided the means to protect the Confidentiality, Integrity, and Availability (CIA) of computers and networks. The Act has been amended in 1994 and 1996.

The CFAA is an anti- hacking Statute and it contains seven sections:-

1030(a)(1) ***Obtaining National Security Information*** - The provisions of this section deals with acts regarding restricted data i.e. whenever a person knowingly accesses government computer to obtain classified information he would be penalized with imprisonment which may extend to 10 years for 1st conviction and upto 20 years for subsequent conviction.

1030(a)(2) ***Compromising the Confidentiality of a computer -*** This section deals with intentional access of computer without or in excess of authorization to obtain information from financial institution. The section aims at protecting computerized credit records and computerized information relating to customers relationship with financial institutions and information on government computer.

The phrase 'without authorization' is used in context of intrusion to computer system or network by a outsider who is seeking access without permission of the owner or authorized person and that of 'exceeding authorization' is used to include within its sphere insiders who are authorized to access but exceeds permission in order to obtain, alter or damage information residing in computer system or network. The issues of without authorization or exceeding authorized access was dealt in case of United States v. Morris[6] It was on 2nd November 1989 when former NSA employee son, Morris released a stealth worm on networked computer. He had miscalculated the pace at which it would spread and damage it will cause. His action caused considerable damage to academic, government and industry computers connected to Internet. The contention which was raised by Morris was that he was permitted to send mail to other computer users and so he should be considered as authorized

[6] United States v. Morris, 928 F.2d 504 (2nd Cir.1991)

user with permitted access to other computers. However the court did not accept his contention and held that he had acted without authorization.[7]

1030(a) (3) ***Trespassing in a Government Computer -*** This section contains provisions regarding intentional and unauthorized access of government computers. Under this section an intruder need not obtain information merely gaining unauthorized access would be treated as violation of integrity of government computer and to make him punishable with imprisonment upto a year and $100,000 fine on 1st conviction and imprisonment of 10 years and $250,000 fine for subsequent conviction.

1030(a) (4) ***Accessing a Computer to Defraud and Obtain Something of Value -*** This section penalises unauthorised access to protected computer with intend to defraud. In this respect were fraudulent use of protected computer exceeds $ 5000 the intruder will be fined $250,000 and imprisonment upto 5 years on 1st conviction and 10 years of imprisonment and fine of $250,000 for 2nd Conviction.

1030(a) (5) ***Damaging a computer*** – The provisions of this section would apply to person who knowingly causes transmission of program, information, code or command and thereby causes intentional damage to a protected computer without authorization. The cases of DoS and DDoS would be penalised under provisions of this section were attacker would be liable for five years in prison for each occurrence.

1030(a) (6) whoever knowingly deals with trafficking in computer passwords with the intention to defraud would liable to imprisonment of 1 year and fine $100,000.

1030(a) (7) ***Threatening to Damage a Computer*** – The section covers cases of extortion threats as against the computer or network owners. The provisions under this section can be invoked only when attacker threatens to launch DoS attack against the victim unless the victim pays the attacker money or thing of value.

United States v. Alexey Ivanov and Vasiliy Gorshkov

In this case, Ivanov and Gorshkov Russian hackers had hacked into Connecticut e-commerce corporation's computer files and stolen the passwords and credit card information for which they were charged under computer fraud and related activity, extortion and possession of unauthorized access devices. They had threatened the corporation with extortion while they were in Russia and moved to dismiss indictment on the grounds that court lacked subject matter jurisdiction, they also contended that as they were in Russia so United States laws were not applicable to them. In this case Russia has extended their cooperation to United States authorities in extraditing them to the United States for trial and Ivanov was held guilty on charges of hacking into 16 companies and served 3 years and 8 months in jail and had to pay $ 800,000 in restitution and Gorshkov was sentenced for 3 years imprisonment and had to pay $ 692,000/- in restitution.[8]

[7] JESSICA R. HERRERA – FLANIGAN, SUMIT GHOSH, CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS 267,268 (Sumit Ghosh, ElliotTurrini 1st ed. Springer 2010)

[8] http://www.csoonline.com/article/2118241/malware-cybercrime/alexey-ivanov-and-vasiliy-gorshkow-russian-hacker-roulette.html

Offences affecting Confidentiality, Integrity and Availability of data under Information Technology Act, 2000 - Comparative analysis of Articles under Council of Europe Convention 2001 and provisions under Information Technology Act, 2000:

Globally, the term Hacking is meant unauthorised access. The reason for gaining unauthorised access depends upon the data found in computers. A hacker may gain unauthorised access to computer for personal monetary gain or for the purpose of stealing confidential commercial or government information. At times the hacker may not only access the data but go to the extent of modifying or altering it to make it worthless.

The provisions regarding hacking are contained in ***Article 2*** of the Council of Europe Convention which means ***illegal access***. However under IT Act, 2000, Section 66 provided a totally new interpretation of the term 'Hacking'. But by amendment to IT Act in 2008 the term has been deleted from s.66 and was substituted by Computer related Offences. The term though deleted the wording of the s.66 finds place under provisions of s.43 (i) of the Amended Act.

The provisions under s.43 provide for civil remedy by way of compensation. But by amendment to IT Act in 2008, if a person dishonestly or fraudulently does any of the acts mentioned in s.43 he would be liable criminally with imprisonment up to three years and fine up to 5 lakh rupees or with both.

Changes brought in the definition of Hacking by ITAA, 2008

The term Unauthorised access is maintained by s.43 (i) which was not clear in the wordings of Section 66 of IT Act, 2000. Yet another point of difference is regarding mens rea. Prior to amendment knowledge of the act that it could cause loss or damage was sufficient to penalize a person even if the act was committed without intention, but, by amendment in order to make a person criminally liable the acts under s.43 must be committed dishonestly or fraudulently.

Cases Registered during 2003- 2013 (All India)

Sr. No.	Offences		Total no. of cases registered 2003-2013
1.	Tampering computer source documents		137
2.	Hacking with computer system		
	i) Loss/ damage to computer resource/ utility ii)Hacking	4864 1645	 6509

3.	Obscene publication/ transmission in electronic Form		3171

Source - NCRB[9]

According to sources of NCRB, the maximum number of cases registered under the Information Technology Act, 2000 are related to Hacking. The total number of cases registered under IT Act, 2000 during 2003 to 2013 were 6509 out of which 4864 of cases were registered under the head of Loss/ damage to computer resource/ utility under S.66(1) and 1645 under S.66(2).

Lacuna in the records maintained by National Crime Record Bureau

Record maintained by NCRB has certain flaws in it which need to be rectified

a) NCRB maintains cyber crime record under 2 heads i.e. cases registered and persons arrested.
I would suggest maintaining data under three heads i.e. Cases registered, Person arrested and Persons convicted of cyber crimes under IT Act.

b) Data with regard to Sec. 66 have been maintained under 2 clauses i.e.
   i) Loss or damage to computer resource/utility
   ii) Hacking
But by amendment to IT Act in 2008 a vast array of offences has been included under Sec.66 of the Act.
Sec.43 has been included in Sec.66. So when offences in Sec. 43 are committed dishonestly or fraudulently they would be penalized under Sec.66 of the Act. So now Sec.66 would be applicable to cases of unauthorized access, Data theft, Denial of access, computer contaminant, Internet time theft, hacking, theft of computer source code, offensive messages, stolen computer resource, Identity theft, cheating by personation, invasion of privacy and Cyber Terrorism.
Since amendment in 2008 no changes have been made in the record of NCRB and it continues to maintain the data under the previous heading and there is no specific data regarding above mentioned individual offences. So we cannot get clear view of offences committed under IT Act, 2000.

Misconception about the term Hacking

There is lot of confusion in understanding the real meaning of the term Hacking, Cracking and Ethical Hacking.

Traditional view

The term Hacking has evolved at MIT, United States of America. Hacking started during the era of 1940s where geeks were curious one to know how systems worked and so unauthorisedly accessed the system to learn how things worked and improvised it.

Changing Concept

[9] National Crime Records Bureau, 2013, Ministry of Home Affairs. Available at: http://ncrb.gov.in, last seen on 07/12/2014

With passage of time malicious hackers started exploiting system for personal gain and so the first Act i.e. Computer Fraud Abuse Act was enacted to restrict the acts of unauthorised access.

The geeks who invaded the system would refer them as hackers and media started covering the incidents by referring acts of unauthorised access for malicious purpose to be committed by hackers. Thus the term started assuming a negative connotation with common man understanding that hacking is a crime and hacker a criminal.

Present Scenario –

1. The CFAA of US is primarily an Anti- hacking Law.

2. The Information Technology Act, 2000 defines hacking as offence under S.66 of the Act.

3. According to the Council of Europe Convention on cybercrime unauthorized access or hacking is an offence under Article 2 of the convention.

The term hacking is widely understood as crime where some countries penalize intentional acts of hacking (unauthorised access) and some mere intrusions into system and legal provisions prohibiting it strengthen the conception of it being crime, though started with good purpose but considering the present scenario hacking is crime. In order to test the understanding about it, field study was done by circulating questionnaire among Officials investigating cyber crimes where question was posed as to whether hacking is crime under Indian law, 100% positive response regarding hacking as crime was found by researcher and when same question was posed to youths, it was found 62.9% have right conception about the term hacking and 37.1% had misconception about it.

Cracking

The hackers of early era make differentiation between the term hacking and cracking. They refer cracking as act which is used for malicious purpose. However they themselves have defined the term and have no reference in law. From the questionnaire which was circulated among youth 57.1% have not heard of cracking and only 42.9% were able to define cracking, however Indian law doesn't recognize the concept of cracking.

Differentiation between hacker and cracker

The contributor in the field of technology for instance Richard Stallman is of opinion that hacking aims at improvising things and so unauthorized access which is gained for malicious purpose should be termed cracking and person associated with it as cracker. . However the Indian Law doesn't make differentiation between hacking and cracking and so no difference between hacker and cracker. When same question was put before youth 91.4% had right conception whereas 8.6% had wrong idea of about the differentiation.

Whether Indian law recognizes ethical hacking?

Ethical hacking has been defined as defensive mechanism that is used to explore vulnerabilities in a system and find solution for these vulnerabilities before a hacker attacks the system. An ethical hacker is a security professional employed by company or

organization to explore the vulnerabilities of a system by using same methods which are used by hacker. 62.9% youth go with this definition and 37.1% are not heard the term.

Cyber crimes are committed by techno savvy people like engineer, computer programmer or who have keen interest in computers. Today's youth find it cool thing to hack into system, play prank or they want to prove that they can break the security of the system. Ethical hacking courses are conducted in India. But this doesn't make any sense where the Indian law has recognised hacking as an offence how ethical hacking can be justified.

To hack is to gain unauthorised access to system. In case of ethical hacking there is agreement between company and ethical hacker where company gives permission to ethical hacker for vulnerability assessment. Once permission is granted by company means there is no unauthorized access and access is one which is permitted so it cannot be termed as ethical hacking.

So we should not blindly follow certain concepts without applying logic. Instead the person who performs vulnerability assessment be termed as network or cyber security expert.

However according to me hacking or cracking both involve gaining of unauthorized access to system which itself is invasion of privacy and cannot be justified because the hackers of earlier era claim so, a base which is morally wrong cannot lead to good future. And this is evident from the present global scenario of Cyber crimes because principles or ethics which were adhered to i.e. freedom of information and free use of technology have been misinterpreted by later generation of hackers who did not believe in exploring things but making use of such unauthorised access to steal the proprietary information for making financial gain.

The hackers of early era also gained unauthorized access to see how systems worked and tried to make alteration to improve the functioning of system. But as there were no law to penalize such unauthorized access or lucky enough that no such charges were leveled on them. But today there are laws which penalize unauthorized access. In this context I would like to refer case of **Aaron Swartz** a software developer, writer and Internet activist. He was founder of Demand Progress which launched campaign against Stop Online Piracy Act and believer of Open source met with undesirable fate on charges leveled against him by MIT Police for breaking, entering & downloading academic journal articles from JSTOR which came under the category of protected computers with imprisonment for 50 years and maximum penalty of $ 1million. Owning to heavy charges leveled against him he committed suicide by hanging on 11th Jan 2013.[10]

The technicalities involved in cyber crimes are highly sophisticated and so dedicated expertise who has updated knowledge of new evolving technology and cyber crimes are the need of day. The evidence involved in Cyber crimes can easily be tampered or deleted or being volatile it can be lost so the crime needs to be investigated on emergency basis if victim is to be given justice in the case.

Article 3 of the convention deals with ***illegal interception***, but the Article fails to describe as to which interception are lawful or unlawful.

[10] En.wikipedia.org/wiki/Aaron_Swartz

Under the Information Technology Act Section 69 confers powers on Central Government or State Government to issue directions for Interception, monitoring or decryption of any information by a computer resource. So far as disclosure of personal information, the same is legal when provider consent to it or when same is required for legal enforcement. But when a person including an intermediary (Internet Service Provider) violates this provision thereby causing loss or gains by disclosing such information without the consent or in breach of contract would be liable to imprisonment up to three years or fine that may extend to 5 lakh or both.

Article 4- Data Interference

Data interference deals with causing intentional damage. As regards the intentional damage under the IT Act s.43 (d) deals with causing of damage to computer, computer system, network, data, database, or programs. This would involve both physical acts of person by causing harm to device or virtually by installation of malware which would cause destruction of data.

Data interference would be applicable to s.43 (i) which deals with destruction, deletion or alteration of information. It would apply in cases of virus, worms which would alter, destroy or delete information stored in computer.

Article 5- System Interference

S.43 (c) which deals introduction of computer contaminant or virus and S.43 (f) which deals with denial of access causes system interference by preventing the legitimate user from operating system or by slowing the system.

Article 6 of Council of Europe convention deals with ***misuse of devices***, there is no provision under Indian Law regarding distribution or sale of hacker tools on Internet

Conclusion

With advancement of Technology the organizations and individuals can hardly cope up with inherent risks involved in it. So, awareness among masses is imperative to deal with new technology crimes. It is necessary that law enforcement authorities are provided updated training and be assisted by resource persons in the field of technology to effectively deal with.

Cyber crimes have assumed global dimension, no nation can remain free from cyber crimes because there is no nation which is out of web of Internet. Due to growing popularity of Internet its usage has increased drastically and cyber security is becoming the main concern of each nation. It is definitely a challenging task for any nation to deal with these forms of crimes alone. Sec. 75 of IT Act provides prescriptive jurisdiction to try any person irrespective of his nationality provided the offence involves computer or computer network situated in India, but in this context it is to be remembered that the same would be possible only if India has extradition treaty with that country.

The Council of Europe convention of 2001 is the first international treaty dealing with cyber crimes. The treaty contains framework which provides for bringing uniformity in substantive and procedural law of parties to convention, for investigation of cyber crime thereby providing power of interception and search of computer resources, and extraditating criminals between the member countries. So if India signs the convention it will be able to exercise extradition treaty with all countries which are party to convention. Till date India is not a signatory to the convention. Considering the transnational nature of cyber crimes international co-operation is

necessary to combat the problem of cyber crimes. So it is imperative that India becomes party to Cyber crime convention.