CHAPTER III
CYBER CRIME AGAINST PERSON
CHAPTER III

CYBER CRIME AGAINST PERSON

This chapter divided into two parts i.e. Part -A & Part- B. Part A deals with the cyber defamation while Part B related with the cyber hacking.

Part A- Defamation

The Internet is a cheap, fast means of international communication of text, sound or image. In other words, an information resource without political or content boundaries; limited only by the extent to which the information providers are willing to disclose their materials and the fruits of their own writing and research. In the present day, web sites displaying information of all kinds are proliferating. These sites are established and controlled by Internet Service Providers (ISPs) or, sometimes, by the company's information technology department. These sites can be accessed through suitable search engines, which will trace and display information to suit the requirements of the searcher. However, not many of the companies are aware of the risks attached with the hosting of a Web site. Who would be held liable, for instance, if an employee clandestinely posts racist, sexist, or defamatory allegations about a competitor on the company's official web site?

---

It is to be remembered that a number of features unique to the internet distinguishes it from any other medium. These features have led to the current re-examination of existing laws relating to defamation, to allow for their possible evolution and ultimately their application in cyberspace.\(^2\) A key feature of the internet is its highly interactive nature. The ease with which users of the internet can access information and communicate with each other has engendered in its users a false sense of freedom in their communications. Accessibility is another feature of the internet, which distinguishes it from traditional print or broadcast media. The relatively low cost of connecting to the internet and even of establishing one's own website means that the opportunity for defamation has increased exponentially. Now, on the internet everyone can be a publisher and can be sued as a publisher.

Another key feature of the internet is that users do not have to reveal their true identity in order to send e-mail or post messages on bulletin boards. Users are able to communicate and make such postings anonymously or under assumed names. This feature, coupled with the ability to access the internet in privacy and seclusion of one's own home or office and the interactive, responsive nature of communications on the internet, has resulted in users being far less inhibited about the contents of their messages resulting in cyber space becoming excessively prone to defamation.

Defamation can be understood as the intentional infringement of another person's right to his good name. It is the wrongful and intentional publication of words or behavior concerning another person, which has the effect of injuring that person's status, good name, or reputation in society. Libel is written defamation and slander is oral defamation. The primary difference is that in libel, damages are presumed, whereas in slander actions, unless the slander falls into a certain category, called slander per se, the plaintiff must prove actual or quantifiable damages.

A person's good name can only be damaged if maligning statements are made to someone other than that person; that is, the defamatory statement must be disclosed to a third person, thereby satisfying the requirement of publication. When determining whether or not defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation.³

Thus the law of defamation places a heavy burden on the defendant. All that a plaintiff has to prove, in a defamation action, is the publication of defamatory matter. The onus then lies on the defendant to prove innocence. Once again, most people are unaware of this burden.

In essence, the law on defamation attempts to create a workable balance between two equally important human rights: The right to an unimpaired reputation and the right to freedom of expression. In a cyber society, both these

interests are increasingly important. Protection of reputation is arguably even more important in a highly technological society, since one may not even encounter an individual or organization other than through the medium of the internet.

3.0 Elements of defamation

➢ The plaintiff must prove publication of the defamatory statement;

➢ The plaintiff must prove that the defamation refers to the plaintiff; and

➢ The plaintiff must prove that the statement is defamatory.

Upon proof of publication, the law makes several presumptions in favor of the plaintiff:

➢ That the statement is false;

➢ That it was published with malice; and

➢ That in the case of libel or slander per se, the plaintiff has suffered damage.

Defences that can be raised against such a defamation action are as:

➢ Truth.

➢ Fair comment: The defendant is allowed to comment on facts truly stated, as long as the comment is fair and the defendant is not motivated by actual malice.

➢ Privilege: On certain occasions, the courts have held that policy and convenience require that a person should be free from responsibility for
the publication of defamatory words. These occasions constitute privileges. Privilege may be absolute, such as statements in the House of Commons or the Courts. It may be qualified, in that it may be lost if the publication is unnecessarily wide or made with malice.

> Innocent dissemination: This last defence is potentially very important in cyber libel.⁴

If a defendant proves that his statements were true and in public interest, then his conduct is regarded as lawful. In addition, if the defendant can show that he had no intention to defame (the plaintiff), then he could avoid liability.

This chapter seeks to throw light on the law relating to cyber defamation and to suggest a legal framework to handle such situations, which is inevitable, especially in the light of the present IT boom in India.

### 3.1 Cyber Defamation: A Socio-Economic Offence

Cyber law encompasses cyber crimes, electronic commerce, and freedom of expression, intellectual property rights, jurisdiction issues and choice of law, and privacy rights. Cyber crimes involve activities like credit card fraud, unauthorized access to computer systems, child pornography, software piracy and cyber stalking. Freedom of expression includes defamation, obscenity issues and censorship. Jurisdiction issues focuses on who makes and enforces the rules governing cyber space.

---

⁴ Ibid.
The definition of what constitutes a crime in cyber space is still being
developed. In the past, the states and federal government defined cyber crime
activities to include the destruction or theft of computer data and programs.
More recently the definition has expanded to include activities such as forgery,
illegal gambling, cyber stalking, cyber defamation etc.

There are several areas on the internet where there is a real risk of
liability for defamation. The fact that a user is "alone" with his computer and
distanced from other users creates a sense of intimacy. There is no
spoken/telephonic conversation or dictated correspondence that would
normally instill some caution. In addition, the notion that the internet is a "free-
for-all" cyberspace where there are no limits or boundaries results in a user's
sense of social norms and propriety generally getting blurred.

The Web results in an instant global publication of information at a very
low cost. Information, which would not normally have been revealed prior to
the dawning of the internet, can now be unearthed by practically anyone.
Intranets are intended to be exclusively used by a company. However,
information from an intranet can be easily downloaded and forwarded by e-
mail or otherwise to third parties. Information posted to a bulletin board can be
accessed by anyone. This means that anyone can place defamatory allegations
on the bulletin board. E-mail users generally tend to treat their correspondence
as a kind of conversation rather than a written interaction. Users forget that e-
mails are stored and can be retrieved as hard copies and that their contents then
cannot be disputed. One message can be circulated to literally hundreds of people. As a defamatory allegation need only be disclosed to one person for publication to be proved, every time e-mail is forwarded to another person, it is published again and an additional cause of action for defamation arises.\(^5\)

The scope of every firm having a cyber presence to liability for defamation is global. Internet sites can be accessed in most countries throughout the world; huge amounts of data can be transmitted simultaneously to several different destinations; and e-mail can be forwarded to an indefinite number of recipients without the original author having any control over the transmission.

While a legal action based on defamation is usually aimed at stopping the defamatory allegations, the harm in most cases has already been done. Consequently, the most important relief claimed in a defamatory action is damages. The amount of damages granted will depend on the nature of the defamation sought and the extent of publication. Furthermore, a defamation claim can be instituted in any jurisdiction in which a cause of action arises. In theory then, a potential defendant to a defamation suit could be sued in respect of a particular defamatory statement in a number of different countries with which it has no connection under any number of different laws with which it is totally unfamiliar. Indeed, a potential plaintiff can choose to litigate in

whichever country has the most favorable laws. Theoretically, every time a third party accesses a defamatory posting on the Internet, publication has occurred.

The global nature of the Internet also raises some interesting procedural questions for the libel lawyer. In traditional libel law there are three different types of defamatory statements:

i) The first is a statement that is defamatory on its face and which is obviously defamatory.

ii) The second is a statement, which contains false innuendo. False innuendo is a defamatory statement that has an inferential meaning, therefore only persons with the necessary contextual knowledge appreciate that the statement is defamatory. Since statements on the internet are published globally, their inferential meanings may vary depending on the geographic or cultural location of the reader or the newsgroups or the Usenet group involved.

iii) The third category is legal innuendo. While not defamatory on their face, these statements are defamatory when viewed together with extrinsic circumstances. Once again, contextual knowledge may render a statement defamatory in one jurisdiction but not in another.

Cyber defamation need not necessarily be directed against an individual victim, but it could be harmful to the whole society. No doubt, at times, it could
be directed against an individual ('victim'), but the criminal act is potentially capable of harming a large number of persons and that is the principal object behind punishing it. In short it is an offence, which affects the health or material welfare of the community as a whole and not merely of the individual victim. Similarly it is also an offence, which affects the country's economy and not merely the wealth of an individual victim, since defamation of a corporate house could even adversely affect its share value.⁶

3.2 Significant aspects of social and economic offence

There are two significant aspects of social and economic offences they are as:

(i) the gravity of the harm caused to society; and

(ii) the nature of the offence.

The gravity of the harm is not easily apparent, but is nevertheless, undeniable. The nature of the offence is peculiar, in the sense that they are planned and executed in secrecy by shrewd and dexterous persons with sophisticated means. The public welfare is gravity affected; but detection is unusually difficult.

Cases of cyber defamation do not fit neatly in the accepted categories of crimes. They represent harm of greater magnitude than the traditional crimes and of a nature different from them. Unlike the traditional crimes, they are not

⁶ Ibid.
in the shape of positive aggressions or invasions. They may not result in direct or immediate injury; nevertheless, they create a danger, which the law must seek to minimize. Hence if legislation applicable to such offences, as a matter of policy, departs from legislation applicable to ordinary crimes in respect of the traditional requirements as to mens rea and the other substantive matters as well as on points of procedure, the departure would be justified.

3.3 Cyber Defamation Position in Other Countries

Defamation laws vary from country to country and in countries such as the Canada, Australia and the United States, it can vary from province to province and state to state. Therefore, plaintiffs may have the luxury of "forum shopping" or choosing the jurisdiction with the laws most favorable to him/her.

3.3.1 Position in US

In the United States, about 75% of defamation lawsuits are filed in state courts, and the remaining 25% in federal courts. A comprehensive discussion of what is and is not libel or slander is difficult, because each state's definition differs. Some states lump slander and libel together into the same set of laws. Some states have criminal libel laws on the books, though these are old laws, which are infrequently prosecuted.7

---

Most defendants in libel lawsuits are newspapers, which are involved in about twice as many lawsuits as are TV stations. Most plaintiffs are corporations, business people, entertainers and other public figures, and inmates. Most states do not allow defamation lawsuits to be filed if the allegedly defamed person is already deceased. None of the states allow the plaintiff to be a group of people.

In the various states, whether by case law or actual legislation, there are generally several "privileges" that can get a libel case dismissed without proceeding to trial. These include the allegedly defamatory statement being one of opinion rather than fact; or being "fair comment and criticism", as it is important to society that everyone be able to comment on matters of public interest. If a defamation lawsuit actually gets to trial, truth is an affirmative defense. Further, if the allegedly defamatory statement is not actually capable of being defamatory, i.e., an insulting statement that does not harm someone's reputation is prima facie not libelous.

*New York Times Company v. Sullivan*⁸ was a U.S. Supreme Court case which established the actual malice standard before press reports could be considered to be defamation and libel; and hence allowed free reporting of the civil rights campaigns in the southern United States. It is one of the key decisions supporting the freedom of the press. The actual malice standard requires that

---

the publisher knows the statement is false or acts in reckless disregard of the truth.

The decision established that for a plaintiff to win a libel ruling against a newspaper, "actual malice" or "reckless negligence" must be proved on the part of the paper if the statement in question is about a public official or public figure. In the case of a private figure, the plaintiff must merely prove negligence.

Prior to the enactment of the Telecommunications Act of 1996, the position in US with regard to cyber defamation was such that the Courts applied the common law definition of "publisher," which held liable anyone who exercised a substantial degree of editorial control over the distributed product. This definition distinguished between a distributor, such as a newsstand or a library, and a publisher, such as a newspaper or book author. Distributors were not to be held liable for the information they disseminated, while those who reviewed content before publication would be held liable. Courts generally analyzed ISP liability under the same standards applied to newspapers and other media.\(^9\)

If a third party published defamatory material on a network and the computer redistributed that material, the owner or operator of the server was liable if:

\(^9\) Supra note 7.
They or their agents knew that the material was defamatory.

They or their agents had reasons to be suspicious that the material was defamatory.

In *Stratton Oakmount v. Prodigy*¹⁰ (1995), the US Supreme Court provided no incentive for online service providers to remove obscene or libelous material from their databases. If any good faith attempt were made to inspect content prior to publication, the online service provider risked liability for any offensive material it missed. This case led to the enactment of the Telecommunications Act of 1996, and was effectively overruled by the said Act.

This Act was signed into law by President Clinton on February 8, 1996, and includes the Communications Decency Act ("CDA") and the Internet Freedom and Family Empowerment Act. The Act recognizes the value of the internet, and declares that the internet has "flourished, to the benefit of all Americans, with a minimum of Government regulation."

**The Act Provides:**

(1) Treatment of publisher or speaker - No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provider by another information content provider.

(2) Civil Liability - No provider or user of an interactive computer service shall be held liable on account of -

---

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

The Act also allows for the enforcement of any State law that is consistent with its provisions. Courts have construed the Act to be a broad defense against libel actions arising out of content provided by a third party, and refused to hold ISPs' liable regardless of whether plaintiffs characterize them as distributor or publisher.

Some argue that Congress acted too hastily in enacting the CDA, and instead should have allowed the courts to apply traditional real space defamation law to cyberspace. By deferring to the courts the law would develop gradually to adapt to the new medium of cyberspace. This would encourage the growth of the internet and simultaneously encourage ISPs to monitor their content. After the CDA, ISPs do not have as much of an incentive to monitor the content of their subscribers' postings.

Liability of ISPs after enactment of the Telecommunications Act can be summarized as follows:
The law has shifted from allowing liability for ISPs even when they tried to screen offensive content, to barring liability for ISPs, even when they promote such offensive content.

The CDA still leaves the problem of the anonymous publisher. The unrestricted global use of the internet makes it easy for someone to publish information about a person without identifying himself. Defamed plaintiffs may be left with no redress when their reputations are damaged or they are harassed by a defendant whose identity is unknown and undiscoverable.

It seems that the CDA has eliminated all liability for internet service providers with respect to libelous postings of its subscribers. Recent case law has given broad protection to ISPs faced with lawsuits for the defamatory postings of their subscribers. Although the CDA was enacted with the honorable goal of promoting ISP self-regulation, it has instead left defamed plaintiffs who do not know the identity of their attackers with no remedy against the very activity the Act was meant to eliminate. Despite the courts' deference to the CDA, the law of cyber-defamation will be forced to evolve to address this problem.

3.3.2 Position in Canada & UK

As with other Commonwealth countries, Canada also follows United Kingdom law on defamation issues. Recently the Supreme Court of Canada in
the case, *Hill v. Church of Scientology of Toronto*\(^{11}\) has reviewed the relationship of the common law of libel and its relation to the Canadian Charter of Rights and Freedoms. The reasoning in this case specifically rejects the actual malice test in *New York Times Co. v. Sullivan*\(^{12}\) citing criticism of it, not only in the United States, but in other countries as well.

Theoretically, damages could be very large as a publication on the internet potentially reaches millions of people. In practice, however, it is unlikely that millions of people will actually view each particular publication. In any event, publication on the internet will generally be larger than in all but the largest print or broadcast media outlets.

A company could also be held liable, as a Web site host/owner, or as an ISP, for any defamatory statement published on its site. If a hacker breaks into a Web site and publishes a defamatory statement, the Web site host or ISP could be held liable. However, if a defendant can show that the publication of the defamatory matter was not intentional, he can escape liability proceedings.

The question that will have to be decided by courts is whether a Web site host can be equated to a distributor of published matter such as a library, or whether it should simply be equated to an institution such as a telephone firm, which is a mere passive conduit for the information which it carries and over which it has no effective control.

\(^{11}\) 1995. 2 S.C.R. 1130.

\(^{12}\) Supra 8.
3.3.3 Position in Australia

Recently, Australia's apex court gave a landmark judgement concerning internet defamation and the related issue of jurisdiction. In the case of *Dow Jones v. Joseph Gutnick*\(^{13}\) Australia's high court has ruled that the financial publishers Dow Jones can be sued in the Australian state of Victoria over an article that appeared on their website. The facts of the case are that Dow Jones & Co. Inc. prints and publishes the newspaper Wall Street Journal and Barron's Magazine. Dow Jones also operates the portal www.wsj.com which is a subscription news site on the internet. Those who have subscribed to the said web site by payment of the subscription charges are entitled to access the same utilizing the user name and password provided by Dow Jones. The on-line edition for 28th October 2000 contained an article entitled "Unholy Gains" in which several references were made to the respondent Joseph Gutnick.

The defamation case was brought by Melbourne mining magnate Joseph Gutnick, who argued that the article could be read on the internet by people who knew him in Melbourne. In his action, Gutnick claimed that the article defamed him by portraying him as a schemer given to stock scams, money laundering and fraud. Dow Jones argued that the court was clearly an inappropriate forum for trial proceedings as the relevant publication took place in the US and that the court had no jurisdiction. Several international media

\(^{13}\) (2002) HCA 56; 210 CLR 575; 194 ALR 433; 77 ALJR 255, (Australian High Court Opinion) via Australasian Legal Information Institute.
companies who also made submissions to the court such as Reuters, News International and Amazon.com backed up that position. The primary judge held that the Australian Court had jurisdiction to try the matter. The case went to the court of appeal of Victoria and finally came up for hearing before the High Court of Australia. It is thought to be the first such decision in the high court of any country to consider the question of jurisdiction and the internet.

Before the High Court, the issue debated was as to where was the alleged defamatory material published? Was it published in Victoria? Dow Jones argued that the publication of the article occurred at its servers maintained in New Jersey in the United States and, therefore, an Australian Court could not assume jurisdiction over the matter.

In a landmark judgement, the High Court of Australia held that the Australian Court indeed had the jurisdiction to try an action for defamation concerning an article, hosted at the servers of Dow Jones in the United States. The Court held that the law of defamation seeks to strike a balance between, on the one hand, the society's interest in freedom of speech and the free exchange of information and ideas and on the other hand, an individual's interest in maintaining his or her reputation in society, free from unwarranted slur or damage.

The majority judgment further held that those who post information on the World Wide Web do so knowing that the information is available to all, without geographical restrictions. The Court further held that defamation is to
be located at the place where the damage to the reputation occurs. It was in the place where any person downloaded the defamatory material that the damage to reputation could be done. Following this principle, the court held that an action for damages for defamation can be continued in Australia against a US web site. This judgement can act as a precedent for all courts in the world as it is that of the Apex Court of Australia, thus enabling the internet to be amenable to worldwide jurisdiction.

3.3.4 Position In India

IPC on Defamation:

Chapter XXI of the IPC exclusively talks about defamation. Section 499 prescribes the offence: "Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person."\(^{14}\) Cyber Defamation, also known as Internet Defamation or Online Defamation, is defamation in the world of Internet and its users. Cyber Defamation is amongst one of the various Cyber Crimes that can take place. Cyber crimes are neither bound by time nor by national boundaries i.e. a person sitting in one corner of the world, can at any time easily cause damage to a person sitting in

\(^{14}\) *Section 499 of the Indian Penal Code.*
another corner of the world within a few minutes. Cyber Defamation in Corporate World can take place in various forms for example a disgruntled employee of a Company may post some defamatory remarks about the Company on a popular blog site or may send some slanderous email, defaming the company or any of its important managerial personnel, to the clients of the company across the globe; a competitor may divert the client and/or customers of a Company visiting the website of the Company to any other website which may give some misleading information about the Company. Unlike other form of defamation Cyber defamation can cause huge damage to a Company in a very short span of time owning to a worldwide accessibility of internet and its ever increasing number of users.

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said . . . to defame that person.

Explanation: 2 It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Section 500 prescribes the punishment in such cases:

Whoever defames another shall be punished with simple imprisonment for a term, which may extend to two years, or with fine, or with both.
Employer's liability

A company can be held liable for the conduct of its employees. If an employee, during working hours, e-mails a defamatory remark about a competitor company to a colleague, the firm could be held liable for defamation even if the employee's actions were not authorized or expressly prohibited.

For instance, in a dispute, which arose in the United Kingdom between the Western Provident Association (WPA) and Norwich Union, it was suggested that Norwich Union staff were spreading e-mail rumors amongst their sales force that WPA was more or less insolvent and under investigation by the Department of Trade and Industry. WPA sued Norwich Union, alleging that the latter was responsible for the communications made by its employees, even though the allegations were made without the instructions or knowledge of the management. The case was settled out of court but it is believed that Norwich Union paid approximately half a million pounds to WPA in settlement.

In fact, Asia's first case of cyber defamation has been filed in India in the case of *SMC Pneumatics Ltd. v. Jogesh Kwatra*\(^ {15} \) Defamatory emails were allegedly sent to the top management of SMC Pneumatics by the defendant, who has since been restrained by the Delhi High Court from sending any form of communication to the plaintiff. This order of Delhi High Court assumes

\(^ {15} \) 1279/2011 Delhi HC.
tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

An important test in determining whether a company can be held responsible for its employees' actions is to decide whether the actions were to the benefit of the company. An employer would be held vicariously liable in case of an employee promoting his own interests.

The Australian judgment could impact freedom of speech of media organizations and expose publishers to legal actions all over the world. The judgment has raised complex global issues regarding internet publications, which could develop over time. The principle enunciated by the Australian Apex court is likely to stand in conflict with emerging jurisprudence relating to jurisdiction. Such an approach is likely to undermine the global nature of the internet, because it could make online publishers cautious and may deny access of their web sites to readers in countries where they fear litigation. This judgment will certainly have an impact on the Indian web publishing industry. It could open up the ground of misuse of law as Indian web publishers would be amenable to defamation laws not only in India but outside.

Further, the offence of defamation as defined in the IPC when extended to cyberspace may not achieve desired results. However, the Australian Judgment
can be cited as a precedent and that will have persuasive value in India. Hence if defamatory material is downloaded by someone in India, that will be enough cause for action even if the servers of such site are located outside India.

3.4 Cyber Defamation and Information Technology Act, 2000

In India Cyber Defamation found in Civil as well as in Criminal proceedings against the accused. Some of the Acts and rules that deal with Cyber Defamation are The Indian Penal Code, 1960, The Information Technology Act, 2000, The Code of Criminal Procedure, 1973 and The Indian Evidence Act, 1872. The Charging Act for prevention of Cyber Crimes in India is the Information Technology Act, 2000. Section 66A of the Information Technology Act, 2000 provides punishment for online Defamation. Section 66A can be read as follows:

6A. 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,
Cyber Crime Against Person

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 three years and with fine.

**Explanation:** For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Section 65A and Section 65B of The Indian Evidence Act, 1872 provides for Admissibility of electronic records as evidence. Some of the sections of Indian Penal Code, 1960 that deal with Cyber defamation are Section 499, 500 and 503.

In case of Tata Sons Limited v. Greenpeace International & Anr. the Hon'ble High Court of Delhi Made the Following Observations:

"It is true that in the modern era defamatory material may be communicated broadly and rapidly via other media as well. The international

---

distribution of newspapers, syndicated wire services, facsimile transmissions, radio and satellite television broadcasting are but some examples. Nevertheless, Internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by the features described above, especially its interactive nature, its potential for being taken at face value, and its absolute and immediate worldwide ubiquity and accessibility. The mode and extent of publication is therefore a particularly significant consideration in assessing damages in Internet defamation cases."

In May 2000, at the height of the dot-com boom, India enacted the IT Act and became part of a select group of countries to have put in place cyber laws. In all these years, despite the growing crime rate in the cyber world, only less than 25 cases have been registered under the IT Act 2000 and no final verdict has been passed in any of these cases as they are now pending with various courts in the country.

Although the law came into operation on October 17, 2000, it still has an element of mystery around it. Not only from the perception of the common man, but also from the perception of lawyers, law enforcing agencies and even the judiciary.

The prime reason for this is the fact that the IT Act is a set of technical laws. Another major hurdle is the reluctance on the part of companies to report the instances of cyber crimes, as they don't want to get negative publicity or
worse get entangled in legal proceedings. A major hurdle in cracking down on the perpetrators of cyber crimes such as hacking is the fact that most of them are not in India. The IT Act does give extra-territorial jurisdiction to law enforcement agencies, but such powers are largely inefficient. This is because India does not have reciprocity and extradition treaties with a large number of countries.

What India needs to do in this backdrop, is to be a part of the international momentum against cyber crimes. The only international treaty on this subject is the Council of Europe's Convention on Cyber Crime, formulated primarily by the European Union. By signing this treaty, member countries agree on a common platform for exchange of information relating to investigation, prosecution and the strategy against cyber crime, including exchange of cyber criminals. At the last count, there are 43 member countries, including the US and South Africa. India is not yet a part of this group and being a member would go a long way in addressing this issue of cross-border cyber terrorism.

The Indian IT Act also needs to evolve with the rapidly changing technology environment that breeds new forms of crimes and criminals. We are now beginning to see new categories and varieties of cyber crimes, which have not been addressed in the IT Act. This includes cyber stalking, cyber nuisance, cyber harassment, cyber defamation and the like. Though Section 67 of the Information Technology Act, 2000 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material
which is obscene in electronic form with imprisonment for a term which may extend to two years and with fine which may extend to twenty five thousand rupees on first convection and in the event of second may extend to five years and also with fine which may extend to fifty thousand rupees, it does not expressly talk of cyber defamation. The above provision chiefly aim at curbing the increasing number of child pornography cases and does not encompass other crimes which could have been expressly brought within its ambit such as cyber defamation.

3.5 Jurisdiction issue in cyber defamation

Internet can been seen as multi-jurisdictional because of the ease with which a user can access a web site anywhere in the world. It can even be viewed as uni-jurisdictional in the sense that from the user's perspective, state and national borders are essentially transparent. The Court in Zippo Manufacturing Company v. Zippo.Com, Inc\(^{17}\) said there is a global revolution looming on the horizon, and the development of the law in dealing with the allowable scope of personal jurisdiction based on Internet use in its infancy.

The developing law of jurisdiction must address whether a particular event in Cyberspace is controlled by the laws of the state or country where the web site is located, by the laws of the state or country where the ISP is located, by the laws of the state or country where the user is located, or perhaps by all of these laws. Some of the jurists are of the view that cyberspace should be

treated as a separate jurisdiction. In practice, this view has not been supported by the Courts or addressed by lawmakers. Cyber jurisdiction issues have been dealt with primarily in the civil courts. Since the advent of *US v. Thomas* and *Minnesota v. Granite Gate Resorts, Inc.* however, cyber jurisdiction issues have begun to be examined in criminal courts as well.

### 3.5.1 Cyber jurisdiction in Civil Cases

In determining whether jurisdiction exists over a defendant, the US Federal courts apply the law of the forum state, subject to the limits of the Due Process Clause of the Fourteenth Amendment. Under Due Process, in order for the court to exercise personal jurisdiction, it must be shown that the defendant had purposefully established minimum contact with the forum state such that the maintenance of the suit did not offend the traditional notions of fair play and substantial justice. In *Bensusan Restaurant Corp. v. King*, the court held that an exercise of personal jurisdiction would violate the protection of the Due Process clause.

Further in the case of *The Hearst Corp. v. Goldberger* the US District Court of the Southern District of New York ruled that nationwide jurisdiction was inconsistent with traditional personal jurisdiction case law, and as a policy matter, it was unacceptable. In *McDonough v. Fallon McElligott* a Federal

---

19 126 F.3d 25 (CA2 1997).
Court in California also refused to exercise personal jurisdiction over the defendant simply because it maintained a web site. The court held that the fact that the defendant had a web site accessed by Californians was not enough by itself to establish jurisdiction.

Further more in *Zippo Mfg. v. Zippo Dot Com, Inc* the court held that a passive web site that only made information available to interested users was not grounds for exercising jurisdiction. A web site that entered into contracts and knowingly and repeatedly transmitted computer files would be properly subject to personal jurisdiction. The issue of jurisdiction should be determined by examining the commercial nature of the exchange and the level of interactivity.

### 3.5.2 Cyber Jurisdiction in Criminal Cases

The question of cyber jurisdiction in criminal cases came to the forefront of attention in early 1996 in *US v. Thomas*, when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. The defendants were convicted by the District Court of Tennessee on federal obscenity charges. They appealed and the appellate court affirmed. There were two premises for their appeal:

1. The federal obscenity statute did not apply to intangible objects like computer Graphic Interchange Format ("GIF") files, and
2. Congress did not
intend to regulate the type of transmissions at issue because the federal obscenity statute did not expressly prohibit such conduct. The Court disagreed ruling that the manner in which the images were transmitted did not affect their ability to be viewed or printed out by members in Tennessee. That the statute should be construed to affect the intent of the Legislators (the Congress) which was to prevent the channels of interstate commerce from being used to disseminate any obscene matter.

In Minnesota v. Granite Gate Resorts Inc., the Court denied the defendant's motion to dismiss for lack of jurisdiction and held that the defendant's advertising on the internet constituted a direct marketing campaign directed at residents of the state of Minnesota, which was sufficiently purposeful to subject the defendant to suit in the forum state.

3.5.3 Cyber Jurisdiction in International Cases

When adjudicating cases involves foreign nationals the courts must balance several factors. On a case-by-case basis, the courts must consider the procedural and substantive policies of other countries whose interests are affected by the court's assertion of jurisdiction. Keeping these policies in mind, the court must then consider the reasonableness of assertion of jurisdiction examined in the light of the interests of the federal government in its foreign relation policies. When extending jurisdiction into the international field, great care and reserve must be exercised. Hence there is higher jurisdictional barrier when litigating against a foreign national.
In order to support personal jurisdiction in cyberspace the courts now require that defendants provide more than mere accessibility to a web site. Some sort of interaction is required. The trend appears to be that information providers must comply with the limitations of the laws wherever the user is located or find themselves subject to the user's state jurisdiction, and its civil and criminal laws. Case law indicates that the courts are inclined to expect the information provider to determine where the user is located and to block access to their site if access is illegal in the users' locale.

Part B - Hacking

The origin of hacking, in the sense of technological exploration and tampering can be traced back to the phone phreakers of the 1960s and 1970s. The word journeyed from being understood as an adventurous achievement in the common parlance during its origin, to the most sought after, uncontrollable and mischievous criminal act in the present IT age. Hacking is described as "interacting with a computer in a playful; and exploratory rather than a goal-directed way." The word "hack" at the Massachusetts Institute of Technology (MIT) usually refers to a clever, benign, and "ethical" prank or practical joke, which is both challenging for the perpetrators and amusing to the MIT

---


community (and sometimes even to the rest of the world).\textsuperscript{25} Thus, hacking, \textit{prima facie} appears to be a harmless activity, indeed it is widely commended and acclaimed as an adventure on wires.

At its core, hacking refers to activities involved in attempting or gaining unauthorized access to IT systems. With the widespread proliferation of computing technology, and the networks connecting it together, systems have come to represent both attractive and readily available targets regardless of whether the motive is idle mischief or something more sinister. As a consequence, hacking has become one of the most recognised and feared threats in cyberspace. For example, from the 671 security executives and law enforcement officials questioned as part of the 4th Annual E-Crime Watch Survey (conducted by CSO Magazine, the US Secret Service, the CERT Program and Microsoft), 26 per cent considered hackers to have been the greatest threat to their organisation over the previous year (placing them at the top of the list, ahead of current and former employees, competitors and foreign entities. Indeed, the same respondents considered that an average of 22 per cent of the security incidents they had experienced in this period had been targeted attacks seeking to hit them specifically.\textsuperscript{26}


Although the general threat is widely recognised, hacking is actually a very broad term, encompassing a variety of potential activities and motivations.

### 3.6 Origin and ethos

In contrast to the commonly accepted use of the term, hacking did not originate in the context of attacks and computer abuse, but rather as an acknowledgement of technical ability. In the early days of computing, a hacker was a hardware or software enthusiast or hobbyist, with the origins of the term being closely linked to the 1960s pioneers at the Massachusetts Institute of Technology (MIT). These early hackers had a genuine belief in the liberating power of technology, and alongside this emerged the so-called "hacker ethic", emphasising principles such as freedom of information and unrestricted access to technology. Such ideas can dearly be seen to be in potential conflict with the concept of security, and from this perspective it is fairly easy to appreciate how the principles could be hijacked and misconstrued; enabling the behaviour associated with hackers to verge into the territories of unauthorized access and intrusion, and then onwards towards disruptive and harmful activities within the compromised systems. As a consequence, looking into virtually any dictionary today will reveal that the common-use definition of a hacker is directly linked to unauthorized activity and breaking security.

The concept of rebelling against authority or a corrupt system is something of a theme in the hacker's self-image. In addition to the aforementioned hacker ethic, there is also the oft-quoted 'Hacker Manifesto'
(also known as 'the conscience of a hacker'), written by The Mentor in 1986. Going somewhat beyond the Ethic's call for information and access to be free, the Manifesto attempts a vehement defence of hacker activities, asserting a level of moral superiority on the part of the hackers compared to those whose systems are being targeted. A few snippets are presented to illustrate the point.

We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore and you call us criminals. We seek after knowledge and you call us criminals. We exist without skin color, without nationality, without religious bias and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

Clearly there will be some who genuinely believe this, but the widespread circulation of the text has potentially allowed it to be a flag of convenience for others who just want to hack but feel the need for some moral justification in doing so.

**Black, white and all the shades in between**

Simply labelling someone a "hacker" is actually a bit simplistic, and a variety of other names can also be used depending upon the sort of things they
are doing. For example, it is common to find reference to 'crackers', in order to denote those acting with an overtly malicious intent and to distinguish them from the more benign and exploratory activities that some like to claim that traditional hackers would engage in. Of course, from a security perspective such a distinction is a fairly moot point; you want to keep unauthorized users out regardless of their possible motivation, because by the time they get in it will be too late to quiz them about it.

Returning to the issue of names, it is also quite common to encounter labels that reflect the hacker's perceived intent, such as black hat, white hat and grey hat. These particular terms reflect whether a hacker is overtly malicious or dangerous (the black hat), using hacking techniques to test and improve security (the white hat), or has unclear or unpredictable behaviour (the grey hat). When considering these particular names, it is worth noting that the legitimacy of the white hat's activity will still depend upon whether they are doing it as a sanctioned activity (i.e. approved by the owner of the system they are targeting), or acting in a self-appointed role without permission. In jurisdictions with related legislation, the latter still represents a criminal act, regardless of how strongly the perpetrator may claim that they are acting as an ethical hacker or a penetration tester.

Other labels tend to reflect the capability of the hacker or the specific type of activity they are engaged in. In the former category would be terms such as 'script kiddie' and 'packet monkey', both of which are used to refer to novice
(wannabe) hackers who lack the technical skill to develop and initiate an attack from scratch but are capable of posing a nuisance by using tools and scripts produced by others. By contrast, labels such as 'hacktivist' and 'phreaker' tend to reflect what the hackers are doing (with hacktivists being those that use hacking methods in pursuit of an activist or political agenda, Handbook of Internet Crime and phreakers being those who seek to explore and experiment with telephone systems).

It can be seen that some of the labels tend to reflect motivation as well as method. With this in mind, it is also worth highlighting that although they often get referred to en masse, hackers are far from homogeneous when it comes to their reasons for entering the fray. For example, those operating at script kiddie level may have been attracted by media coverage and Hollywood-style glamorization of hacking, and a consequent desire to be part of the same world. Conversely, others will be drawn in by a genuine fascination with the technology and what can be done with it. For others, it is the challenge of beating the system, or the people that are trying to protect it. And for an increasing proportion of perpetrators, hacking is just a means to an end; attacking or compromising a system is seen to represent the easiest or most effective way of getting a desired result (be it to cause damage, attract publicity, or steal money etc.).
3.7 Who is a hacker?

Steven Furnell regards hackers as the "anti-heroes of the computer revolution". This is in reaction to the title of a book, *Hackers: Heroes of the Computer Revolution* written by Steven Levy in 1984 depicting the change in attitude over the last two decades. Steven Furnell says thus, Levy's book was not about computer criminals, but the pioneers of 1950s and 1960s computing to whom the term "hacker" was originally applied as a mark of respect for their skills. In the 1960s, hackers were the dedicated software and hardware gurus, and the term largely referred to persons capable of implementing elegant, technically advanced solutions to technologically complex problems. Hackers then were very gifted programmers and, when Levy wrote this book, he was reflecting upon a different era. In the new millennium, the moniker implies something rather different and is commonly used to refer to persons who gain unauthorized access to systems and data. At the extreme arc a subset (often distinguished by the term crackers) that perform openly malicious actions upon the systems they enter, such as deleting files, modifying data and stealing information. Such activities would be frowned upon by the original hackers of the 1960s, who regarded technology as a means of liberation rather than a tool for causing damage and destruction.27

27 Supra, note 1, p-140.
Hackers are basically regarded as learners and explorers who want to help rather than cause damage and who often have very high standards. A hacker as according to traditional opinion is someone who does some sort of interesting and creative work at a high intensity level which includes anything from writing computer programs to pulling a clever prank that amuses and delights everyone. However, controversy regarding use of the term "hacker" continued for long as some regarded hackers as respectable programmers or gurus and are of the opinion that the term should not be used to refer to those who abuse and misuse the system. Taylor after an extensive research outlines Steven Levy's (1984) hacker "generations", detailing the "true" hackers of the 1950s and 1960s, who were seen as the pioneers in their field, hardware hackers who were responsible for opening access to hardware during the 1970s and game hackers of the 1980s who generated games for the hardware. In all, the hackers as identified by Sceven Levy in the four decades as mentioned above, none of these are regarded as harmful activators or lawbreakers. In fact, they were the heroes until 2001 when Taylor updated the typology of hackers, added three more types of hackers but he unlike, Steven attributed "illegality" to them, did away with the difference between hackers and crackers, and described a hacker or cracker as an individual who illicitly breaks into other

30 Supra, note 1, p-140.
computer systems, much the same as Wall's cyber spy. Even microserfs are those individuals who once belonged to, or are still associated with hacker groups but work within corporate structures, such as Microsoft. Thus, apart from media revelations, the word "hacker" is defined in various dictionaries in the following words;

A computer fanatic, especially one who through a personal computer breaks into the computer system of a company, government, etc,

*Coliins English Dictionary (3rd Edn.) 1994*

A (computer) hacker is a person who hacks into other people's computer systems.

*Cambridge International Dictionary of English, 1995;*

A person who uses computers to gain unauthorized access to data.

*New Oxford Dictionary of English, 1998*

A skilled and enthusiastic computer operator, especially an amateur, an operator who uses his or her skill to break into commercial or government computer or other electronic systems.

*Chambers Dictionary, 1998*

A person who uses computer for a hobby, especially to gain unauthorized access to data.

*Dk Illustrated Oxford Dictionary, 1998*

---

In nutshell it can be said that the common element in all the definitions laid emphasis on the activity of the hackers and termed them as “unauthorized”. Consequently, one can say with certainty that in today's terminology, the word "hacker" is synonymous with a cyber criminal and it no longer has the exclusive connotation of being expert code writers of the first generation hackers. Irrespective of the fact that hackers regard themselves as harmless intruders, and some of them known as Utopians even believe they are helping society by demonstrating the vulnerabilities in the system, the cyber specific legislation of almost all the countries has included them (or their activity) as totally illegal causing harm to others by damaging their data and thus causing wrongful loss to many, whether or not it is causing wrongful gain to hackers or any other person. The reason for this considerable change in the mind of lawmakers owes to the fact that the legal history of the passing decade has shown that the technique employed by hackers is the technique which is commonly used to commit most of the cybercrimes. Moreover, hackers of the information age are known by a good variety of names such as cyber terrorists, cyber warriors, hackivists, script kiddies, warez doodz, etc.

31 Terrorists who employ hacker-type techniques to threaten or attack against systems, networks, and/or data. As with other forms of terrorism, cyber terrorist activities are conducted in the name of a particular political or social agenda. The underlying objective will typically be to intimidate or coerce another party (e.g. a government). Steven Fumell, Cybercrime: Vandalizing the Information Society (Addison-Wesley, 2002) 44.

34 Persons employing hacking techniques in order to attack computer systems that support vital infrastructure, such as emergency services, financial transactions, transportation and communications. This essentially related to the application of hacking in military and warfare contexts. Ibid.
which are all violators of law. Hackers are the specialists in computer technology, skilled in bytes and masters of the keyboard. They are also accomplished code-writers who sell their skill for money. Not only that they are curious browsers but also some of them are disgruntled and dissatisfied cyber engineers ready to trade in their skill. Just as indigenous people may be turned into soldiers, so can crackers (hackers) be turned into cyber terrorists.\(^3^8\) They usually work in groups as the technical job requires a human chain to be successful in the exercise. These hacker groups are numerous and cyber attacks mainly originate in places like the former Eastern bloc, China, and Libya, from where they can control thousands of machines simultaneously.\(^3^9\) These hacker groups often have political objective but mostly they work for profit.\(^4^0\) Thus, yet another factor which draws a line between the commendable hackers of

\(^{35}\) Hackers who break into computer systems in order to promote or further an activist agenda. Incidents such as the defacement of websites are very often linked to these individuals. *Ibid.*

\(^{36}\) If individuals with fairly limited hacking skills who rely upon scripts and programs written by order more competent hackers. Hackers of this type typically cause mischief and malicious damage, and are generally viewed with scorn by more accomplished members of the hacking community. Such individuals may also be referred to as "packet monkeys" or "code kiddies".

\(^{37}\) A subclass of crackers, who obtain and distribute illegal copies of copyrighted software (after first breaking any copy protection mechanisms, if appropriate). The spelling used is representative of a common form of hacker slang—in this case the two words, when written properly, are "Wares Dudes". More commonly these individuals are known as software pirates. *Ibid.*


yesteryears and the work-for-profit hackers/crackers of today is evident from the terrorist-hacker liaison.\footnote{As it remains closely guarded secret, frequent news of the liaison between cyber terrorist and hacker does not come. However, it is reported that the Indian separatist group Hartal ul-Ansar attempted to purchase military software from hackers in 1998. In March 2000, Aum Shrinikyo Cult organisation reportedly had contracted to write software for up to 80 Japanese companies and 10 government agencies including Japan's Metropolitan Police Department but there were no computer attacks related to these contracts. Dorothy Denning, "Cyber Terrorism", 24-8-2000, \url{http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc}.

3.8 Hacking Without Intention to Commit any Further Crime

There are various kinds of hackers. The word "hacker" is used to describe all of these.\footnote{"Cyberpunks & Hackers", at \url{http://www.lacessor1.net/~ajberwar/ajhpmle.htm}.

3.8.1 Code Hackers - They know computers inside out. They can make the computer do nearly anything they want it to.

3.8.2 Crackers - They break into computer systems-Circumventing Operating Systems and their security is their favourite pastime.

3.8.3 CyberPunks\footnote{The first use of the term "cyberpunk" is credited to Gardner Dozois, who was the editor of Isaac Asimov's Science Fiction Magazine in the early '80s. He got it from file title of a short story by Bruce Bethke, "Cyberpunk". The author William Gibson is probably the most widely known cyberpunk author. He wrote the trilogy Neuromancer, Count Zero, and Mona Lisa Overdrive. His world is set in the near future describing a rather dark world where corporations rule the world, and information is power. This world is populated with cyber jocks, super-hackers who run the web of the future to steal information.} - They are the masters of cryptography.

3.8.4 Phreakers - They combine their in-depth knowledge of the Internet with mass telecommunications systems.
Hackers are becoming a menace so uncontrollable that even the largest companies in the world are finding it difficult to cope up with their incessant attacks.

Some hackers "enjoy" cracking systems and gaining access to them, they do not intend to commit any further crime. It is a question of debate whether such act in itself constitutes an offence or not. They may not be brought within the ambit of existing laws if they are interpreted conventionally. The act of such a hacker can perhaps, most appropriately, be considered in the light of laws relating to criminal trespass.

Trespass in common language means to go on another's property without permission or right. Though it is ordinarily a civil wrong, if trespass is committed with criminal intention, it is treated as criminal trespass. The ingredients of the offence of criminal trespass have been laid down under Section 441 of the Indian Penal Code. The object of making trespass a criminal offence is to keep the trespasser away from the premises of individuals so that one may enjoy his/her property uninterrupted by any intruder.⁴⁴

An act, to constitute trespass under Section 441, IPC, must comprise one of the following:

---

There must be an unauthorized entry into or upon property against the will of the person in possession; or

- There must be an authorized entry lawfully obtained into or upon property but unlawfully remaining therein.

Also, such entry or unlawful stay must be with an intention to commit an offence or to intimidate, insult or annoy the person in possession of the property.

In applying the section to hacking on the Internet, the primary question that needs to be answered is whether websites are "property". The common law action of trespass to real property served to establish and preserve the very notion of "property" in land. Many of the words used to describe websites have a basis in real property: the word "site" itself is one, as are such expressions as "home" pages, "visiting" Websites, "travelling" to a site and the like. This usage suggests that the trespass action might appropriately be applied to websites as well. That analogies to real property trespass can be made does not suggest, however, that they should be made. The fundamental issue is whether the treatment of websites as property makes sense in light of the justifications for the institution of property generally.45

---

45 Four strands of property theory-Locke's natural rights, Bentham's utilitarianism, Hardin's "tragedy of the commons," and Radin's "property as personhood" turn out to yield strong justifications for treating Web sites as property and hence for the application to them of the common law of trespass.

Thus, as trespass actions are grounded in the idea of protecting an owner's control over real property which is just a particular species of "property", there is no inherent reason that a website could not be considered a species of "property". Hence, there is no reason for not allowing a cause of action for "trespass to websites".

The next important question arises when a hacker has no intention to commit any further crimes. The question is whether such hacking is, enough to constitute intimidation or annoyance? Under Indian law it has been clearly laid down in *Smt. Mathri v. State of Punjab*\(^{46}\) that for establishing the offence of criminal trespass it is not enough to merely show that the person entering upon the property of another had knowledge that his act would cause annoyance. The rule that a person must be presumed to intend the natural consequences of his act is not a binding rule, if any other intention can be shown. This interpretation may be problematic dealing with crimes on the Internet.

### 3.9 Hacking-specific legislation: the UK, the US and India

Though originally speaking, hacking reflected dexterity at the keyboard and there was total absence of mens rea in the exercise, and the pioneers in this field were considered to be the gifted ones. In the present age, the legal machinery is geared up to tie the noose around the hackers as they started using their skill for illegal purposes. Even though there is absence of mens rea, at

\(^{46}\) AIR 1964 SC 986.
times, the financial loss caused is so enormous that the legal response to it could not be done away with. Thus, sui generis legislation has been adopted to tackle the threat to the security of computer systems, their integrity, confidentiality and availability.  

In the UK, the Computer Misuse Act, 1990 became law on 29th August 1990. The direct origins of the Act are found in the Law Commissions Report on computer misuse. The Act was formulated with the sole purpose of securing the computer system from the unfounded ambitious intentions of the hackers which were showing the criminals the path to misbehave and make money by breaking into the systems of others and at the same time remaining unnoticed and uncaught by law enforcement agencies. Under the 1990 Act, the offence of hacking is crystallised into different sections starting from Section 1 which contains the basic hacking offence and regards "causing a computer to perform any function" as the actus reus of the offence under Section 1. The mens rea of the offence under Section 1 consists of the following two elements:

1. There must be intent to secure access to any program or data held in any computer.

---


49 S. 17(1) of the same Act defines "function" to include alterations or erasure, copying or moving data, using it or producing output from the computer.
2. The person must know at that time that he commits actus reus because the access he intends to secure is unauthorized.

According to Section 1(2.) of the Act, the intent need not have to be directed at any particular program, data or computer.

The term "actus reus" was interpreted in *R. v. Sean Cropp,* where the prosecution could not succeed in getting the defendant punished as the facts of the case were such in which the offence was allegedly committed in a stand-alone computer where the defendant is said to have "keyed in certain commands to the computerized till granting himself a substantial discount". After the arguments, it was accepted by the court that Section 1 (1) (a) required "that a second computer must be involved". It was held that, had the legislators intended the section to apply to a single computer, the wordings would have been "causing a computer to perform any function with intent to secure access to any program or data held in that or any other computer", while the present section contains only the underlined phrase. The interpretation was, however, rejected by the Court of Appeals which preferred the plain and natural meaning. It will not be out of place to mention here that the Council of Europe Convention permits Member States in matter of offence of "illegal access" to limit the offence to "exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system".

---

50 Snares Book Crown Court, 4-7-1991.
As truly remarked by Ian, interpretation of Section 1 as given by the lower court would have seriously limited the scope of the Act as the instances of hacking are no longer the exclusive work of outsiders but it is commonly carried out by the insiders or the employees within the organization. The Act also suffers from the lacuna of not defining the most important term, "computer". However, Smith argues that a narrow view of what constitutes a computer must be adopted.

Section 2, Intent to commit a further offence This section requires commissions of an offence under Section 1 along with the intent to commit, or facilitate the commission of a further offence. Such a further offence is any other offence for which punishment is fixed by law and which may be an offence under any other Act. According to clauses (3) and (4) of Section 2, the access under Section 1 and the further offence need not have been intended to be carried out at the same time and it also does not matter if the further offence was in fact impossible.

Scope of Section 2 came up for discussion in R. v. Farquharson, where the defendant and his co-defendant Ms Pearce were prosecuted. Here, though Ms Pearce was the employee who accessed the computer system for obtaining the mobile telephone numbers and codes, and the defendant was prosecuted for

---

51 Audit Commission Report, "Ghost in the Machine: An Analysis of Fraud Si Abuse (1398)" which found that nearly 25 per cent of frauds were committed by staff in managerial positions. p. 303.


53 Croydon Magistrates' Court, 9-10-1993.
obtaining the mobile telephone numbers and codes necessary to produce cloned telephones, it was Ms Pearce who was prosecuted under Section 1 offence and the defendant was found to have committed the unauthorized access required for the Section 2 offence, though he never touched the computer himself. The construction of Section 2 is such that the phrase regarding "the commission of further offence" is likely to dominate the prosecutions held under it and the perpetrator's act of unauthorized access may be sufficient to find a prosecution for an attempt to commit the further offence.\(^5^4\) Sections 1 and 2, of the Act are applied in several cases such as \(R. \, v. \, Pearlstone\)\(^5^5\) in which an ex-employee used his former company's telephone account and another subscriber's account to defraud the computer-administered telephone system and place calls to the US; and \(R. \, v. \, Borg\)\(^5^6\) where an investment company analyst was accused of establishing dummy accounts within a "live" fund-management system. The alleged "further offence" was expected to be fraudulent transfers into the dummy accounts. The abovementioned cases were all individual cases of hacking where the common and non-professional defendant applied various techniques of hacking. But the first classic hackers were prosecuted under the Act in \(R. \, v. \, Strickland\)\(^5^7\) and \(R. \, v. \, Woods\)\(^5^8\), where the defendants were given six-month jail sentences for conspiracy to commit offences under Sections 1

\(^5^4\) Supra, n. 19, p-305.

\(^5^5\) Bow Street Magistrates' Court, April 1991.

\(^5^6\) 1969 SCR 551.

\(^5^7\) 2013 NLCA 65(CanLII).

\(^5^8\) Southwark Crown Court, March 1993.
and 3 of the Computer Misuse Act, 1990. The defendants' activities were said to have caused damage, valued at £1, 23,000, to computer systems ranging from those of the Polytechnic of Central London to NASA. The opinion of the Judge was expressed in following words:

There may be people out there who consider hacking to be harmless, but hacking is not harmless. Computers now, form a central role in our lives containing personal details...it is essential that the integrity of those systems should be protected and hacking puts that integrity in jeopardy.\(^{59}\)

Thus, such a judicial pronouncement lays stress on the fact that with the increasing involvement of computers in our lives, hacking can no longer be regarded as a skill or art; in fact, it is the emerging criminal misconduct.

Slowly the weight shifted towards tightening the legal noose around the hacker's neck. In the US too, complacency prevailed regarding hackers' activities but "In 1990, there came a nationwide crackdown on illicit computer hackers, with arrests, criminal charges, one dramatic show trial, several guilty pleas, and huge confiscations of data and equipment all over the United States"\(^{60}\).

The Computer Fraud and Abuse Act, 1986 regulates several criminal activities on the Net apart from "unauthorized access" in order to obtain

---

\(^{59}\) As the prosecuting authorities mistakenly chose to prosecute for conspiracy rather than for a charge under the Computer Misuse Act, 1990, the defence argument that one of the co-defendants, Bedworth lacked the required mens rea for a charge of conspiracy because he was an obsessive hacker. This led to his acquittal by the court. *Supra*, n. 19, 305.

sensitive information such as defence-related information and financial and consumer credit records, among other things. Trafficking in passwords for computers used by or for the US government is also barred. The Act in Section 1030(a)(5)(A) also prohibits the transmission of "a program, information, code or command to a computer or computer system" with intent to damage, or cause damage to, or to withhold or deny the use of, a computer, computer services or network, information, data, or program. Such transmission is also prohibited if done with reckless disregard of a substantial and unjustifiable risk of the same effect.

India, being a member of the information society, not only relishes the fruits of technological advancements but like its any other counterpart, it also exposes itself to breach of security and has been a victim of it for umpteen times and even important government and scientific installations were not spared. India thus, woke up to check the menace.

61 18USC S. 1030(a)(6).


63 There are several cases registered or unregistered related to hacking, in India. Few examples are: ZeeTV.com, goznexEJob.com, etc. and a notorious group of Pakistani hackers called G-Force during 2001 hacked many websites of Indian organisations, for example, Indian Science Congress, Asian Age Newspaper, National Research Centre, Agricultural University of Maharashtra, IIM (Ahmedabad), IIT (Chennai), Indian National Information Technical Promotion (New Delhi), etc. Then, in 2002, the website of Assam Tourism Department was hacked by unknown hackers. Here the hackers replaced most of the photographs of tourism interest with pornographies. Perhaps, the most shocking instance of hacking in India is, when a 15-year old American boy with a strange name "t3k-9", hacked into the Mumbai based Bhabha Atomic Research Centre (BARC) computer network soon after the Pokhran nuclear tests, during May 1998. He passed on the information to his friend named "Iron Logik", an 18-year old immigrant from Serbia, and placed the list of 800 BARC login names and passwords to a hacker...
Thus in India, in the unamended IT Act, 2000, the offence was separately defined under Section 66. The offence in this section partakes both the elements of traditional crime, i.e. mens rea and actus reus. Section 66 is replaced by a new section by the IT (Amendment) Act, 2008 (10 of 2009). Instead Sections (i) and (j) have been inserted in Section 43 of the Act which reads as follows:

Section 43 Penalty for damage to computer, computer system, etc.—

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(ii) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

Section 43 is to be read with the newly substituted Section 66 which says that

Section 66 Computer related offences. If any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with

channel. Again, a group of hackers who call themselves "Armagedon" gained access to an Indian Bio-Medical Research Facility during 1998 and stolen the test results and internal memos on the possible effects of nuclear tests on the country's environment and civilian population.


64. Hacking with Computer System.—(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

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

65. Inserted by virtue of S. 32 of the IT (Amendment) Act, 2008 (10 of 2009).
imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Explanation, For the purposes of this section,

(a) the word "dishonestly" shall have the meaning assigned to it in Section 24 of the Penal Code (45 of 1860);

(b) the word "fraudulently" shall have the meaning assigned to it in Section 25 of the Penal Code (45 of 1860),

Thus the offence of hacking is, though by name, not there in the statute book but it has been qualified with the necessary mental element. An act, which "destroys, deletes, or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means", is punished criminally if it is done "dishonestly" and "fraudulently". These words clearly denote the element of mens rea required for the crime and the words; destroys, deletes, alters and affects; are the verbs which contain the element of actus reus.

The term "dishonestly" is defined in Section 24 IPC in the following words:

S. 24. Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Thus, the term "dishonestly" has specialized meaning denoting thereby that "unless there is wrongful gain to one person, or wrongful loss to another,
an act would not be dishonest". Thus, a mental condition will not fit into the expression of "dishonestly" unless the intention is to cause either wrongful loss to someone or wrongful gain to someone; the IPC thus, explaining the terms wrongful gain says that wrongful gain is achieved where the gain is by unlawful means of such a property to which the person gaining is not legally entitled and wrongful loss denotes the losing of such property by unlawful means to which the person losing has legal title. Thus, the amended Section 66 makes it necessary for all the acts under Section 43 to be done by which wrongful gain is caused or wrongful loss is caused. Moreover, the section also uses the term "fraudulently" which is defined in Section 25 IPC, in the following words:

S. 25. *Fraudulently* A person is said to do a thing fraudulently if he does that thing with intend to defraud but not otherwise.

The terms "fraud" and "intend to defraud" are not defined in the IPC. The term denotes an element of deceit and secrecy, and actual or possible injury.

It is notable here that in the new amendment like the similar provisions of the UK and the US, the Indian law too, has not explicitly used the term

---


67 S. 23 IPC, p-18.

68 Supra note 37.

"hacking" in its provision though it imports the concept by using the terms "deletes, destroys, diminishes its value", etc. Moreover, the phrase "unauthorized access" as used in Section i of the Computer Misuse Act, 1990 of UK and in 18 USC Section 1030(a) (6) of US, is avoided in Section 66 of the IT Act, instead the terms "dishonestly" and "fraudulently" have been introduced which is the typical wording of the various sections of the IPC. This explains the particular type of mental element or mens rea required for a particular type of offence which means that accessibility is not of so much importance as the effect of it, namely, causing wrongful loss or damage to the public or any person. In fact, it has been made the element of the offence of hacking. The wording of Section 66 will also avoid situations which arose in UK in *R. v. Sean Crapp*, 70 in which the offence was committed by the defendant in a stand-alone computer and the defence succeeded in raising the point that Section i of the Computer Misuse Act, 1990 is constructed in such a phrase that it is legally not possible to bring the defendant's activity under the mischief of the said section.

3.10 Case situation in India (Illustration)

Suppose A, an employee, while having a deal with an outsider, keys in certain commands into the computer through which he solicits certain discounts and financial favours for himself causing wrongful loss to his employer, at the same

---

70 Snaresbrook Crown Court, 4-7-1991.
time. Here, what is the offence caused by A? Can A be prosecuted under Section 66?

If one goes by the wordings of Section 66, A's keying of commands into the computer is covered by the word "alters" thereby forming the required actus reus. Mens rea is evident from causing wrongful gain to himself and at the same time causing wrongful loss to his employer. Here, though the number of computers used is only one but A is guilty of hacking as all the ingredients of the section are satisfied, namely, intention or knowledge to cause wrongful loss or damage and destruction, doing the act dishonestly, deletion or alteration of information residing in a computer. Under the Indian law, mere unauthorized access is not an offence, at least not under Section 66. Here, as A is an employee, hence (unless he shows that he was not authorized to access the computer in question), his accessibility is not unauthorized. Had his accessibility been "unauthorized", the other proper section to bring an action against A is Section 43(1) of the IT Act which read with Section 66 makes the act an offence punishable under Section 66. This is the section which regards accessibility as a wrongful act and where it has to be done either dishonestly or fraudulently. In the given situation, thus, A is successfully prosecuted under Section 66, if he does it to cause wrongful gain or wrongful loss to anyone or has done the act with intent to defraud. If found guilty then A is made liable to pay damages by way of compensation and he is also, if mens rea is proved,

---

liable to be punished with imprisonment for term up to three years or with fine which may extend to five lakh rupees or with both [S. 66].

The Indian law deals with accessibility of protected system in a particular manner and separately under Section 70 of the IT Act which is made an offence. A difference is thus seen between unauthorized accessibility of a computer, computer system or computer network and unauthorized accessibility of a "protected system" under Section 70. In Section 43(a), one has to prove mens rea as envisaged under amended Section 66 to make it a punishable offence and if it is done without mens rea then it entails only damages by way of compensation; Section 70 punishes the offender with unlimited fine plus with a maximum sentence of 10 years.

3.11 Hacking and criminal trespass

Hacking is often regarded as cyber trespass which is the invasion of private space on the Internet by a hacker. The term "trespass" implies an act without authority or right which again implies absence of allowing or permission by the person in charge. Criminal trespass denotes the act of trespass with an intention to commit a crime which can be trespass to a house, land or "property". In applying the term "trespass" to hacking, the primary

---

72 S. 70(3). Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

question that needs to be answered is whether websites are "property." Four strands of property theory Locke's "natural rights", Bentham's "utilitarianism", Hardin's "tragedy of commons" and Radin's "Property as Personhood" turn out to yield strong justifications for treating web-sites as "property" and hence, for the application to them of the common law of trespass. Thus, while almost all the legal systems of the world regard trespass to real property as a tort or offence, there are equally good justifications to regard trespass to virtual property as an offence as the trespass actions are grounded in the idea of protecting an owner's control over real property which is just a particular species of "property."

If hacking is understood as criminal trespass, it should be kept in mind that Section 66 of the IT Act, which deals with the offence of hacking, contains mens rea as an ingredient, the question then comes up whether a hacker can also be prosecuted under Section 441 IPC? The object of making trespass, a criminal offence is to keep the trespasser away from the premises of individuals so that one may enjoy his/her property uninterrupted by any intruder. Section

---


441 requires the following ingredients\textsuperscript{78} to constitute the offence of criminal trespass:

(1) Entry into or upon property in the possession of another.

(2) If such entry is lawful, then unlawfully remaining upon such property.

(3) Such entry or unlawful remaining must be with intent,

\begin{enumerate}
\item[(a)] to commit an offence; or
\item[(b)] to intimidate, insult, or annoy any person in possession of the property.
\end{enumerate}

As advocated by Ratanlal, "property" in this section means immovable corporeal property, and not incorporeal property such as a right of fishery\textsuperscript{79} or a right of ferry.\textsuperscript{80} The judicial opinions, coming in an age where the Internet or the concept of virtual property perhaps did not exist, have maintained their relevance to date. Thus, while dealing with Internet trespass or cyber trespass, application of Section 441 IPC will not serve any purpose as the third ingredient of criminal trespass under the section, namely, the intent to commit an offence or to intimidate, insult or annoy is neither always clear nor is it easy to prove such an intent on the Net. Moreover, entry, access or hacking by the offender even though at times is not malevolent, yet it is harmful for others and hence, regarded as an offence. With the enactment of Section 66 of the IT Act, destruction, deletion, or alteration of information on the computer, etc. and


\textsuperscript{79} Empress v. Charu Nayiab, ILR (1877) 2 Cal 354.

\textsuperscript{80} Muthra v. Jaauhir, ILR (1877) 1 All 527.
doing so either dishonestly or fraudulently is regarded as an offence whether or not there is "an intention to commit an offence" as required by the third ingredient of Section 441 IPC. Mere tampering with the information residing in a computer resource is regarded as an offence. Section 43 being a cyber trespass specific legislation is an apt one to deal with trespass on the Net if it is done without mens rea.

3.12 Comparative study

Hacking is no longer an art; rather it is a criminal act as declared by almost all the laws of the world. The oldest law in this field was formulated by the US in 1986, when the Internet and network computers were out of the boundaries of developing countries like India. Even for some years, the UK was lagged behind and it was only in 1990 that the Computer Misuse Act became law on unauthorized access.81 The IT Act in India deals with the offence of hacking in a conditional manner without using the term. The substituted section requires that the destroying, deleting, etc. in a computer resource should be done dishonestly or fraudulently to make it an offence under Section 66 read with Section 43(i). The comparative study of the offence of hacking and unauthorized access is done summarily under the following heads.

81 The direct origins of the Act are found in the Law Commission's Report on computer misuse published in October 1989. In December 1989, Michael Colvin introduced a Private Member's Bill, with the tacit support of the government, closely following the English Law Commission's recommendations. The primary motivation for government support was possibly a belief that if the UK did not follow the example of many of its European partners, then the UK's position in the European information market could suffer. Ian Walden, Chap 9 "Computer Crime" in Chris Reed Sc John Angel (Eds.), Computer Law (5th Edn. Oxford University Press, 2003) p.303.
3.13 Legal position in the UK, US and India

It is interesting to note that while the UK and the US legislate specifically to deal with the offence of hacking, both the countries avoid a definite definition of hacking, as such the relevant Acts do not even use the term "hacking". India follows suit and in the substituted Section 66 of the IT Act, the same pattern is followed though under the original Section 66, the term "hacking" was used. The Computer Misuse Act, 1990 basically deals with computer vandalism and criminal activities on the Net, presents three new categories of offence: unauthorized access to computer material [S. 1]; unauthorized access with intent to commit a further offence [S. 2]; and unauthorized modification [S. 3]. Of these, in Section 1, offence of unauthorized access to computer material is the basic hacking or cracking offence. The Computer Fraud and Abuse Act, 1986 of US meant to combat hacking, prohibit unauthorized access in order to obtain sensitive information.

As the offence of hacking cannot be committed without a computer, the US Act defines computer as an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device.

The UK Act, however, is criticised for not including the definition of computer but the Law Commission of UK found general support for the view that to attempt such a definition would be "so complex, in an endeavor to be

---

82 Ibid.
all-embracing, that they are likely to produce extensive argument."\textsuperscript{83} However, the Indian law, on the subject, gives the definition of "computer" in its general clauses definition in Section 2, (i) of the Act in the following words: 2 (i) 'computer' means any electronic, magnetic, optical or other highspeed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

The definition is exhaustive and the words used here are very similar to the words used in the above definition of the US Act. In comparison with the US definition, this definition includes the term "manipulations" in addition to the word "facilities". The Indian definition also seems to be broader, as apart from computer, it uses the word "computer system and computer network".

**Main law provisions**

*Mens rea element* The element of mens rea is found in Section i of the UK Act and in Section 66 of the IT Act as well. In both the sections, intent and knowledge on the part of the defendant is required to make him guilty of the offence of hacking. The offence, therefore, is essentially an intentional one. Here, the notable point is that in the traditional hacking activity, intent to cause harm\textsuperscript{84} or damage is opposed to the hacking ethic.\textsuperscript{85} Does it mean that if today,

\textsuperscript{83} Ibid.
\textsuperscript{84} "We are not doing any harm"; "We do not intend to do any harm"; "We're not altering or destroying anything, so that must be okay"; These are some of the opinions given by the hackers about themselves as these quotations are taken from the commentary made in a UK Channel Four documentary a few years ago. This represents the true picture of the mind of a hacker. Nevertheless, the fact cannot be denied that the apparently harmless activities of
not a criminal but a glorified, true hacker, with pure bona fides makes an unauthorized access (UK and US laws), or diminishes the value and utility, or affects injuriously the information residing in a computer resource (IT Act), can he still be prosecuted under the above laws? He has no mens rea; how can he be brought under the mischief of above provisions? Can he take the defence of pure intentions? Then what is his liability? And what about the harm he caused through his adventurous and benevolent intentions? The suggestions to book such hackers under the liability of criminal trespass is still a debatable point as even under criminal law, whether it is in India under Section 441 IPC or elsewhere, a mala fide intention is a prerequisite which is, however, denied by traditional hackers. These law provisions will be put to test when they are examined and applied in law courts. However, so far as UK and US are concerned, some landmark judgments have already started revealing the

the hackers are causing havoc. Furthermore, their mere presence in the system may steal CPU cycles, memory, disk storage and network capacity that may degrade or prevent other essential activities (any form of real-time control system would be an example of where this might be significant). A relevant example can be cited here from 1997, when US space shuttle astronauts were put at risk when a hacker broke into a NASA computer system and overloaded it such that medical communications between the shuttle and the NASA center were impeded. These systems continually monitor the astronaut's heartbeat, pulse and medical condition and, at the point when the hacker struck, the shuttle was in the process of attempting to dock with the Mir space station. The hacker, however, was unaware of this context and, from his perspective, the unauthorized presence in the system was exploratory and harmless. In reality, of course, it was anything but harmless and disrupted the system at a crucial time. Steven Fumell, Cybercrime: Vandalizing the Information Society (Addison-Wesley, 2002), p. 50.

85 "And you call me criminal...Yes, I am a criminal, my crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for". Quoted from The Conscience of a Hacker: The Mentor written on 8-1-1986.

86 In UK, in R. v. Bean Cropp [Snaresbrook Crown Court, 4-7-1991] where question arose whether S. 1 offence can be committed on stand-alone computers. In Director of Public Prosecutions v. Bignell, (1998) 1 Cri App R 1, question arose about the extent of unauthorized accessibility, etc. These decisions limited the scope of the Act.
lacuna present in these provisions. The suggestion here is to impute strict liability on hackers.

It is the keyword in the sections dealing with hacking both in the UK and US laws. But the adjective which prefixes it is "unauthorized". The word "unauthorized" raises several questions and often it becomes difficult for the prosecution to prove in case of access by employees that whether the access was unauthorized. The burden in such cases falls on the prosecution to show that the accused knew that "access of the kind in question" was unauthorized. In *Director of Public Prosecutions v. Bignell*, the accused police officers accessed the Police National Computer (PNC) via an operator for personal purposes though they were authorized to access for policing purpose only but they accessed it for some personal purpose. The Divisional Court where the matter went for a second appeal upheld the view of the Crown Court that the Computer Misuse Act, 1990 was primarily concerned "to protect the integrity of computer systems rather than the integrity of the information stored on the computers ...". Later, in *R. v. Bow Street Magistrate and Allison (AP), Ex p. US Govt.*, it was felt that the court's acceptance of Bignell would seem to perpetuate the uncertain jurisprudence under the 1990 Act, hence, Lord Hobhouse recognises that the concept of authorization needs to be refined. In

---

87 Under S. 17(5) of the Computer Misuse Act, 1990, access is considered to be "unauthorized" if
(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

88 (1998) 1 Cri App R.I.

89 (1999) 3 WLR 620.
Indian law, the word "access" or "unauthorized access" is not used in Section 66 but in the opening words of Section 43, the words used are "if any person without permission of the owner or any other person who is in charge of a computer, computer system, or computer network", which in reality equivalent to "unauthorized access". The IT Act deals with such "unauthorized access" in Section 43(a) where the activity renders the doer criminally liable only if it is done "dishonestly" or "fraudulently" as required by Section 66.

Plaintiff's liability In some law provisions, the liability of the defendant is at certain points coextensive with that of the plaintiff. It is often required to prove whether the plaintiff applied sufficient security measure in his systems. In the UK, during the passage of the Computer Misuse Bill, an attempt was made to add a provision whereby hackers would be able to offer a defence if computer users had not implemented security measures. This is to say that the concept of "due care and attention" to avoid the breach of security is to be read into the concept of "unauthorized access", i.e. failure to take appropriate measures will give the defendant a point of defence. This view is, however, incongruous as security measures either does not come handy or they are pretty expensive to be applied by each and every computer owner. In this respect, the

90 See, Standing Committee C, 14-3-1990. The following amendment was proposed by Harry Cohen MP: "For the purposes of this section, it shall be a defence to prove that such care as in all the circumstances, was reasonably required to prevent the access or intended access in question was not taken". Ian Watden, Chap 9 "Computer Crime" in Chris Reed & John Angel (Eds.), Computer Law (5th Edn. Oxford University Press, 2003) 306.
liability of the hacker must be sole and exclusive keeping in view the magnitude of the damages caused by their inadvertence.

**Penalties**

Laws of various countries have different provisions while dealing with the offence of hacking. While UK and US have prescribed the punishment for hacking activity under the name of "unauthorized access", India has declared it to be a criminal offence only if it satisfies the prerequisites of dishonesty or fraud. Punishment under the Indian law is stringent as when the accused is made criminally liable, he is punished with imprisonment up to three years, or with fine which may extend up to five lakh rupees, or with both [S. 66]. As regarding penalty for damage to computer, computer system, the defendant is liable to pay damages by way of compensation to the person so affected.