Cyber Law: Provisions and Anticipation

Taraq Hussain Sheakh
Lecturer in computer
Sciences at Govt. Degree College
Poonch, J&K, INDIA

ABSTRACT
Cyber law is a term used to portray the permissible issues related to the use of communication technology, predominantly "cyberspace", i.e. internet. It is less a distinct field of law in the way that property or contact are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an endeavor to amalgamate the challenges presented by human bustle on the internet with bequest system of laws applicable to the physical world. The growth of Electronic commerce has propelled the need for vivacious and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of electronic commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law. This research paper tends to strike the drastic and immensely growing problem of cyber crime by taking some universal essentials and stature and also shows their preclusions.
Keywords-: Cyber law, Cyber crime, Cyberspace, Fakesm.

Introduction
In today's epoch of rapid expansion Information technology is encircling all walks of life. These technological developments have made the alteration from document to paperless communication possible. We are now creating the new Principles of tempo, efficiency, and exactness in communication, which has become elucidation for boosting innovations, inventiveness and rising overall productivity. Computers are comprehensively used to store confidential data of political, social, economic or delicate nature to bring gigantic benefit to the society. The hasty enlargement of Internet and computer technology globally has led to escalation of internet related crimes. These crimes have virtually no boundaries and may affect any country across the globe. Thus there is a need of consciousness and of obligatory legislation in all the Countries for the anticipation of computer related crime. Globally internet and computer based commerce and communication cut across defensive restriction, thereby creating anew domain of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. This novel periphery, which is made of screens and passwords, separate the "Cyber World" from the "real world" of atoms. Territorially based law making and law-enforcing authorities find this new environment deeply threatening.

Need of Cyber Law
When internet was developed, the founding fathers of internet hardly had any inclination that internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the mysterious nature of the internet, it is possible to engage into variety of criminal activities with the impunity and people with intelligence, have been grossly misusing this aspect of the internet to perpetuate criminal activities in cyberspace.

Importance of Cyber Law
Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws are a very technical field and that it doesn't have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. It is imperative to sense the unenthusiastic impacts of internet and to give check to the Cyber crime [7].

As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain, to the time you setup your website, to the time you conduct electronic commerce transactions on the said site, at every point of time, and there are various cyber law issues involved[3]. You may not be bothered about these issues today because you may feel that they have not impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyber law for your benefit.

Evaluation
Cyber law is constantly being evolved. As new and new opportunities and challenges are surfacing, Cyber law, being a constantly evolving process, is suitably modifying itself to fit the call of time. As the internet grows, numerous legal issues arise. These issues vary from domain names, to intellectual property rights to Electronic Commerce to Privacy to Encystations to Electronic contracts to Cyber crime to Online Banking to Spamming and soon. The list is very long. Whenever the Cyber crime evolves and the mind of cyber criminals appraise to do cyber related crimes, the Cyber law also evaluates to fix the crime [6].

Today, the awareness about Cyber law is beginning to grow. Many technical experts in the beginning felt that legal regulation is not necessary. But with the rapid growth of technologies and internet, it is crystal clear that no activity in the internet can remain free from the influence of Cyber law. Publishing a Web page is an excellent way for any commercial business or entity to vastly increase its exposure to millions of persons, organizations and governments world-wide. It is that feature of the internet which is causing much controversy in the legal community.

Objectives
As internet has grown in our Country, the need has been felt to enact the relevant Cyber laws which are necessary to regulate internet in India. This need for Cyber laws was propelled by numerous factors.

Firstly, India has an extremely detailed and well defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is The Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on[4]. However the arrival of the internet signaled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic and cultural scenario of that relevant time. Nobody then could really visualize about the internet. Despite the brilliant acumen of our master draftsmen, the requirements of cyberspace could hardly ever be anticipated as such, the coming of the internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws.

Secondly, the existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in Cyber space. In fact, the practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging Cyberspace, without enacting new Cyber law. As such, the need for enactment of relevant Cyber laws.

Thirdly, none of the existing laws gave any validity or sanctions to the activities in Cyberspace.

Fourthly, internet requires an enabling and supportive legal infrastructure in tune with times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of internet, can only be possible if necessary legal infrastructure compliments the same to enable its vibrant growth.

Cyber Crimes

Cyber Crime is undeterred by the panorama of arrest or trial, cyber criminals around the world lurk on the Net as an universal hazard to the financial health of business, to the trust of their customers, and as an emerging threat to Nation's security[19].

Common types of Cyber Crimes may be broadly classified in the following groups:-

1) Against Individuals: -

A. Against Person: -

- Harassment through e-mails.
- Cyber-stalking.
- Dissemination of obscene material on the Internet.
- Defamation.
- Hacking/cracking[1].
- Indecent exposure.

B. **Against property of an individual: -**

- Computer vandalism.
- Transmitting virus.
- Internet intrusion.
- Unauthorized control over computer system.
- Hacking /cracking.

2) Against Organizations: -

a. Against Government, Private Firm, Company, Group of Individuals: -

- Hacking & Cracking.
- Possession of unauthorized information.
- Cyber terrorism against the government organization.
- Distribution of pirated software etc.

3) Against Society at large: -

- Pornography (especially child pornography).
- Polluting the youth through indecent exposure.
- Trafficking.

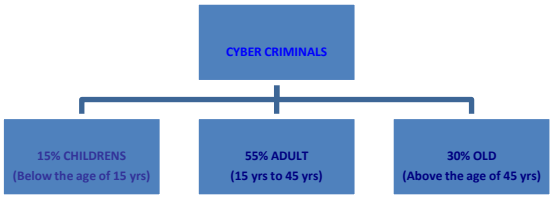

Figure 1.1 Cyber crimes on the basis of age group

A general comparative analysis of different age groups has been taken (Children, Adult, and Old people) by taking the five types of crimes i.e. Obscene material, Fakesm, Indecent exposure, Pornography and Hacking. It shows that the children are more prone to fakesm i.e. Making fake Id and less towards the Indecent exposure shown in the figure 1.2, while the old group people sensitive to Hacking and showing less stick to fakesm shown in the figure 1.3 and the Adult group of peoples stick towards pornography and shows less attraction towards fakesm shown in the figure 1.4

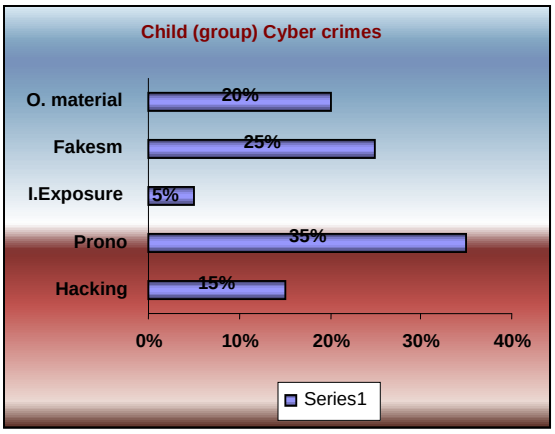

Figure 1.2 showing Cyber crimes by children

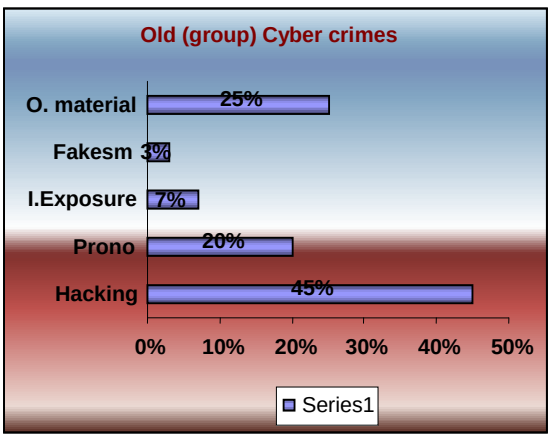

Figure 1.3 showing Cyber crimes by Old people

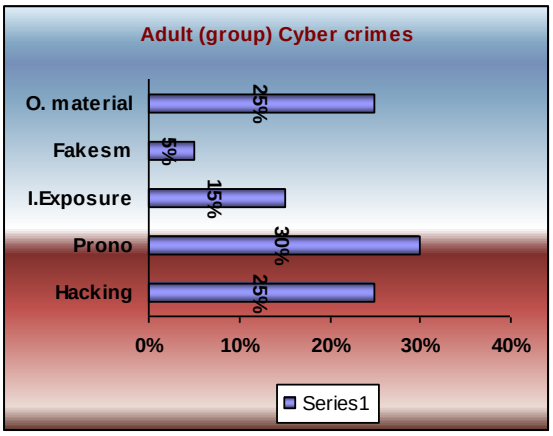

Figure 1.4 showing Cyber crimes by Adult

Conclusions

.

The culmination may, therefore, be disastrous that computer-related crime is a genuine, growing phenomenon. Additionally, a steady augment in number of such crimes in this region is expected which demands for better attention of lawmakers detail and depth study will be further needed which is entirely a liability if not the Internet will use appropriately. Stringent and austere laws should be made and will be implemented honestly is also the dire need of the hour. The law of the Internet has already emerged, and we believe can continue to emerge with individual users voting to join the particular systems they find most pleasant. A general data has been taken which shows the criminal behavior of the different age groups. We need to redefine Cyber Legal processes in this new dynamic context which should be imposed and look forward to throws light into the practical utility of Cyber Crime. Finally, the Cyber Law defined as a considerate group conversation about core values and distinct benefits to the society will persist.

This paper futuristically engross preventing the cyber crime of different age groups by inculcating psychological nature of Cyber Crime created by people (shows the data in the figures) as well as ensure new and modified version of Cyber laws which is emphatically dire need of the problem .

References

[1] Cyber Crime: Practices and Policies for Its Prevention, The First International Conference on Interdisciplinary Research and Development, 31 May - 1 June 2011, Thailand byAjeet Singh Poonia, Dr.Awadesh Bhardwaj, Dr. G.S Dangayach.

[2] Computer Vulnerabilities, Eric Knight, CISSP, Electronic Edition, March 2000, release 4.

[3] Granville Williams

[4] Duggal Pawan

[5] Nagpal R. – What is Cyber Crime?

[6] www.unpan1.un.org/intradoc/groups/public/documents

[7] www.cyberlawassociation.com.

[8] www.cyberlawonline.com.

[9] www.asianlaw.org/cyberlaw/library/index.html.

[10] www.smartsmart.in.

[11] www.indii.org/cyberlaw.aspx.

[12] Cyber Laws: provisions and preventions by Taraq Hussain.

[13] www.free-articals-searc.com.

[14] www.cyberlawcentral.com.

[15] www.thisbooksshop.com

[16] www..csdms.in.

[17] www.cyberlawenforcement.org.

[18] www.cyber.law.harvard.edu.

[19] Zhou, J.; Heckman, M.; Reynolds, B.; Carlson, A.; Bishop, M. (2007). Modeling network intrusion detection alerts for correlation. ACM Transactions on Information and System Security (TISSEC), Volume 10, Issue 1, pp.-1-31.

[20] Sommer, R.; Paxson, V. (2003). Enhancing byte-level network intrusion detection signatures with context. In: Proceedings of the 10th ACM conference on Computer and Communications Security, ACM, pp. 262-271.

[21] Pouzol, J. P.; Ducass, E. M. (2002). Formal specifications of intrusion signatures and detection rules. In Proceedings of the Computer Security Foundation Workshop.

[22] Kruegel, C.; Vigna, G. (2003). Anomaly detection of web-based attacks. Proceedings of the 10th ACM conference on Computer and communications security, ACM Press, New York, NY, USA, Pages: 251 – 261.

[23] Ghosh, A. K.; Wanken, J.; Charron, F. (1998). Detecting Anomalous and Unknown Intrusions against Programs. In Proceedings of the Annual Computer Security Applications Conference (ACSAC'98), pp.-259-267, Scottsdale, AZ.

[24] Cyber Crime and Punishment, Archaic Laws Threaten Global Information December 2000, by McConnell International.