Overview to Cyber-Crimes

Anchal Mittal and Yugansh Mittal

***Abstract*—** The forms of Cyber-crimes have undergone significant metamorphosis due to the advancement of technology and tremendous growth observed in the internet user base globally. Cyber-crime being a complex problem encountered by countries worldwide, raises various complications, snags and difficulties due to its borderless and anonymous nature.

In this work, the emphasis is to sensitize the readers towards the newfangled category of Cyber-crimes and essential judicial precedents. The mainstream focus in this work is India with references from other Countries.

***Keywords*—** Cyber-crime, defamation, obscenity and privacy.

I. Introduction

TODAY the virtual environment has germinated to new levels of growth and efficiency. With the increased dependency on paperless processes and digitalization trend cyber-crimes have stemmed out as one of the more obscure form of crime.

Any crime committed in the cyber-space, or the internet or e-platform are known as Cyber-crimes. A formal definition of Cyber-crime is still not devised or established. Attention was drawn towards this inadequacy by The United Nations in its manual, Prevention and Control of Computer related crimes and later by the Council of Europe. It appears that the Indian Information Technology Act, 2000 and the major cyber laws in the US and UK do not have a concreate definition for Cyber-crimes [12].

The abacus was presumed to be earliest form of a computer initially introduced in India, Japan and China around 3500 B.C [13] but the era of modern computers began with Charles Babbage.[1] Subsequently, the digitalization in 1980's which expanded it wings in 1990's made storage of large amount of data uncomplicated and effortless. The first cyber-crime recorded took place in the year 1820.

In India internet was originally made available through ERNET and for commercial purpose by Videsh Sanchar Nigam Limited (VSNL) and in 1997 the first Indian online banking facility was launched by ICICI bank [14]. However, this ramification had unbolt doors to mass crimes like hacking, frauds, personality in-personation, spamming, etc. and crimes relating to intellectual property rights.

Today this phenomenon of computers and internet technology have come a long way, and cyber-crimes have delineate a whole new species of crimes.

Cyber-crime can affect any individual or organization, be it small or large organization, the risk revolves around 24/7 and can be executed from any part of the world. The landscape of Cyber-crimes is dramatically changing globally and cyber criminals are using more sophisticated techniques to commit cyber-crimes. In some scenarios, it gets rather hard to quantify the cyber threats and its impact on livelihood and businesses. Today the cyber-crimes are not only potentially targeting at stealing information rather disrupt businesses, identity theft and conduct espionage. In such a situation considering security to be robust is a myth, however, individuals and organizations must incorporate security measures and be wise with data security over the internet.

This work emphasizes on the contemporary cyber-crime rather than the traditional cyber-crimes like hacking, frauds, spamming, etc.

II. Cyberspace Statistics

Statistically, around 40% of the world population has an internet connection today however in 1995, it was as low as 1%.

The number of internet users has increased tenfold from 1999 to 2013.[2] According to a study by Internet World Stats based on the internet users, facebook subscribers and population statistics for 35 countries and regions in Asia in June 2014, 45.7% of internet users were from Asia. India is ranked second in Asia's list for top internet countries base on Asia's mobile and broadband reports.[3] The table in Fig 1 shows the growth of internet users as on July 2014 at 7.9%.

Year (July 1)	Internet Users	Users Growth	World Population	Population Growth	Penetration (% of Pop. with Internet)
2014[4]	2,925,249,355	7.9%	7,243,784,121	1.14%	40.4%

Fig 1: Growth of Internet Users

Anchal Mittal is with Law Department, Shree Guru Gobind Singh Tricentenary University (SGT) University, Gurgaon, Haryana, India. (e-mail:mittalanchal28@gmail.com).

Yugansh Mittal, is with Law Department, Shree Guru Gobind Singh Tricentenary University (SGT) University, Gurgaon, Haryana, India. (e-mail:yuganshmittal1@gmail.com).

[1] http://wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber%20crime.pdf

[2] For further details refer *http://www.internetlivestats.com/internet-users/#tren*.

[3] For further details refer *www.interentworldstats.com/stats3.htm*.

[4] Estimate for July 1, 2014

Source: Internet Live Stats (elaboration of data by *International Telecommunication Union (ITU)* and *United Nations Population Division)*

Fig 2 represents the ratio of progress on updating laws to tackle cyber-crimes worldwide which shows only 19% of cyber-crimes related laws are updated worldwide.[5]

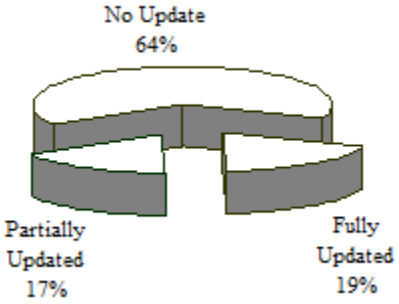

Fig 2: Extend of progress on updating Cyber-crimes law
Source: Dr. Amita Verma, Cyber Crime and Law, Central Law publication, 1st ed., 2009.

According to a survey conducted by KPMG the perception of cyber-crimes and frequency of cyber-attacks in India has seen good rate of increase. Fig 3 shows that 81% of the population surveyed considers Cyber-crimes as a major threat, moreover 51% deem to be easy target of cyber-crimes.[6]

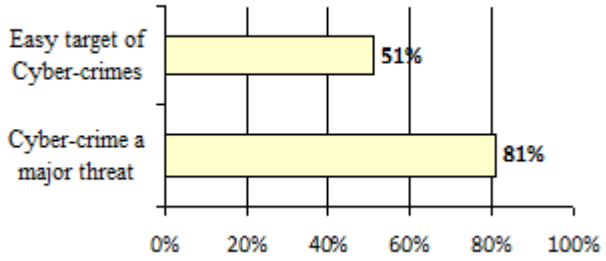

Fig 3: Perception of Cyber-crimes in India
Source: Cyber-crime survey report 2014, by KPMG in India

Fig 4 represents the survey result conducted by KPMG in India done to ascertain frequency of cyber-attacks in India. 49% of the respondents had experience cyber-crime in the last year from the date of survey.[7]

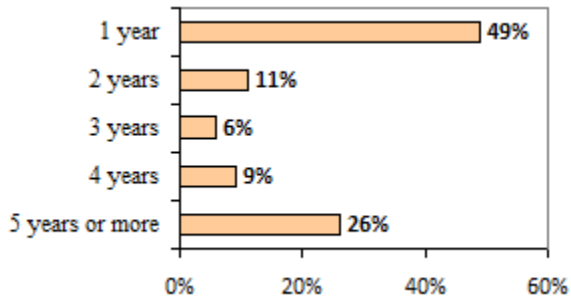

Fig 4: Frequency of cyber attacks
Source: Cyber-crime survey report 2014, KPMG in India

The various statistical result show increase penetration of internet and Cyber-crimes in India. Hence legislation, implementation and infrastructure have to be made robust so that Cyber-crimes are not serious threat to national security, economy and people of India.

III. Cyber-Crimes

A. Cyber Defamation

To discern the meaning of Cyber defamation the traditional term 'defamation' needs to be examined. Defamation is defined as 'an act of harming the reputation of another by making a false statement to a third person'. Any false communication, intentionally either published or publically spoken, that injures another's reputation, goodwill or name or defames a person amounts to defamation. Such imputation might occur on the internet as well. If the alleged defamation involves a matter of public concern, the plaintiff is constitutionally required to prove both the statements falsity and the defendant's fault.[8]

This form of crime doesn't cause loss to physical property or life howbeit cause injury to the reputation of a person. The defamatory content may be expressed orally or can be in written form.

Cyber defamation draws meaning from contemporary term defamation since specific meaning to cyber defamation is still undeveloped. The author is of the view that cyber defamation is 'any imputation happening on the internet by visual representation or content published over the internet or email sent containing material which defames or harms the reputation of any individual'. Moreover, defamation not only spreads in the area of origin or dissemination but travels with the content wherever it is circulated, accessed and viewed. An individual can be effortlessly defamed worldwide over the internet due to the borderless territory of the virtual world. The defamatory material available over the internet can be viewed by vast internet audience at the same time. Cyber defamation not only victimizes an individual rather it can victimize a whole community or society at large.

[5]Dr. Amita Verma, *Cyber Crime and Law*, Central Law publication, 1st ed., 2009.
[6]For more information refer *https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf.*
[7]*ibid*

[8] Black's Law Dictionary, 9th Edn., Thomson Reuters, 2004

In *Tata Sons Limited vs. Greenpeace International & Anr*[9], the Indian court observed that "Communication via the Internet is instantaneous, seamless, inter-active, blunt, borderless and far-reaching. It is also impersonal, and the anonymous nature of such communications may itself create a greater risk that the defamatory remarks are believed". In this case the plaintiff claimed that by the impugned online game "TURTLE Vs. TATA" the Defendants were spreading defamatory remarks and statements, although interim order was refused to the plaintiff.

The statutory provisions governing crime relating to defamation in India would deduce from section 499[10]-502 of the Indian Penal Code, 1860. However, prior to quashing down of section 66A[11] of the Information Technology Act, 2000 done in the landmark judgment *Shreya Singhal vs. Union of India*, this provision applied to cyber defamation.

Under the Information Technology Act, 2000, a victim of cyber defamation was eligible to lodge a complaint directly with the Cyber-crime investigation cell. These cells are specialized investigation cells dedicated to look into Cyber-crimes. However, the scope for crimes of cyber defamation is now restricted to the provisions of Indian Penal Code, 1860 after Supreme Court of India quashed section 66A of the Information Technology Act, 2000.

Nevertheless, cyber defamation has not been considered in the scope of section 66A of the Information Technology Act, 2000 according to the view in *Shreya Singhal vs. Union of India.* Further in this judicial precedent section 66A of the Information Technology Act, 2000 has not been deemed itself with injury to reputation. In fact injury being the basic ingredient of defamation, something being grossly offensive and annoy or be inconvenient to somebody, without affecting his reputation doesn't amount to defamation. It was therefore argued that section 66A is not aimed at defamatory statements at all.

Moreover, defamation is a non-cognizable offence whereas under section 66A of the Information Technology Acts, 2000 the offence was made cognizable. This adds to the view set out in Shreya Singhal case for non-application of section 66A. While section 66 A has been quashed, the provision is inapplicable to be used in cases of cyber defamation but still relevant to interpret what's cyber defamation.

According to an Indian lawsuit, Google (the petitioner) was not allowed to claim relief under section 79[12] of Information Technology Act, 2000 against dissemination of defamatory material through its online medium. It was further stated that Google did not make any effort to block the defamatory content or stop dissemination. So, it makes the role of intermediary's relatively clear in case of cyber defamation happening through their platforms or medium.[13] They cannot simply shrug off their duty against cyber defamation by this provision as the content is channelized through their mediums which must be monitored for any form of Cyber-crime. Apart from above artefact the Indian code stated the essence of publication in defamation. In *Bennett Coleman & Co. vs. Union of India*[14], it was held that publication means dissemination and circulation. Hence, communication of defamatory statement to the concerned person exclusively does not amount to publication.

Cyber defamation is not restricted to any particular means, it can take place in any mode or manner. From signs, visual representation, sending-receiving emails, online bulletin board chat rooms, music downloads, audio files, screaming video, digital photography to SMS, MMS, photographs and videos on mobile phones are considered instances of defamation in electronic form. But cyber defamation is still to see considerable convictions.

B. Cyber Obscenity

Obscenity has always been a precarious issue as it has a close nexus with morality and civility be it traditional form of obscenity or cyber obscenity. It is difficult to truly ascertain what obscenity stands for or to find a circumscribable boundary for the term as there is no concrete definition of the word in any Indian law. Cyber obscenity is one facet of this term of obscenity.

In India certain test for obscenity laid down by the Supreme Court of India are appurtenant to cyber obscenity as well.[15] The law relating to obscenity is primarily enshrined in the Indian Penal Code, 1860 and the Information Technology Act, 2000, i.e. section 292 Indian Penal Code, 1860 and section 67 Information Technology Act, 2000. The definition of the term has been interpreted by courts by value of 'tests' for obscenity. The earliest test was laid down in England the *Regina v. Hicklin*[16] as "Whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influence and into those hands a publication of this sort may fall. It is quite certain that it would suggest to the minds of the young of either sex or even to persons of more advanced years, thoughts of a most

[9] MANU/DE/0220/2011

[10] Section 499 of IPC Act Defines Defamation - 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.

[11] Section 66A of IT Act- Punishment for sending offensive messages through communication service, etc. -Any person who sends, by means of a computer resource or a communication device,-(a) any information that is grossly offensive or has menacing character; or(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or(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.

[12] Section 79 of Information Technology Act, 2000-Intermediaries not to be liable in certain cases.

[13] *Google India Pvt. Ltd. represented by its Managing Director and Mr. Sailesh Rao, S/o. Nagaraja S.Rao vs. Respondent: Visaka Industries Limited, rep. by its Authorized Signatory Sri R. Rajanikanth, S/o Shri R. Varadarajulu and State of A.P., rep. by the Public Prosecutor,* MANU/AP/0209/2011

[14] (1972) 2 SCC 788

[15] http://www.nalsarpro.org/CL/Modules/Module4/Chapter-2.pdf.

[16] (1868) 3 QB 360

impure and lascivious character". Hicklin test postulated that a publication has to be judged for obscenity based on isolated passages of a work.

Further in *Ranjit D. Udeshi vs. State Of Maharashtra*[17], while upholding the constitutional validity of section 292 IPC, the court took a modified version of the Hicklin test that "obscenity without a preponderating social purpose or profit cannot have the constitutional protection of free speech and expression, and obscenity is treating sex in a manner appealing to the carnal side of human nature, or having that tendency. Such a treatment is offensive to modesty and decency but the extent of such appeal in a particular book etc. are matters for consideration in each individual case."

Moreover, in *Miller vs. California*[18], the US Supreme Court set out a three-prong test for obscenity "(a) whether "the average person, applying contemporary community standards" would find that the work, taken as a whole, appeals to the prurient interest, (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value". This is the most commonly used test in India.

In *Aveek Sarkar & Anr vs. State Of West Bengal*[19], the Apex Court of India has applied the "contemporary community standards test" rather than "Hicklin test" to determine what "obscenity" is. The court were also of the view that Hicklin test is not the correct test to be applied, it was noted that "Only those sex-related materials which have a tendency of "exciting lustful thoughts" can be held to be obscene, but the obscenity has to be judged from the point of view of an average person, by applying contemporary community standards." Thus, this would take into consideration the changing times and understanding of the society. The contemporary community standards test was further endorsed in subsequent judgment of the Supreme Court of India in 2015[20].

The Information Technology Act, 2000 has covered offences relating to cyber obscenity in the form of section 66E and section 67. Section 66E prohibits the publishing or transmission of the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person. This would include acts of unauthorized publication of personal images. Section 67 provides for the punishment for publishing or transmitting obscene material in electronic form if they publish material "which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely". Further, though publication or transmission of obscene material may be illegal, but mere possession, browsing or surfing through obscene content is not an illegal activity. In 2008, the Delhi High Court included the proliferation of a sexually explicit MMS clip within the meaning of section 67 and the listing as obscene[21]. Section 67A prohibits publishing or transmission of sexually explicit act or conduct. This is a more specific section to deal with "sexually explicit' content, while section 67 is more generic and has a wider scope. Section 67B specifically deals with publishing or transmitting of material depicting children in sexually explicit act in electronic form, it criminalizes all kinds of online child pornography.

Courts have held and it is noted that the concept of obscenity varies from country to country depending on the standards of morals of the society[22]. Lady Chatterley's Lover, the novel in dispute in Ranjit D. Udeshi itself can be seen as an example, the book was considered obscene in India but was not in other parts of the world such as Canada or England.

Today cyber obscenity has become money making or one can say lucrative area of business in Internet for criminals.

C. Privacy in Cyberspace

The right to privacy can be best interpreted to mean the right to be left alone and the right of a person to be free from unwarranted publicity[23]. Black's Law Dictionary says that the terms "right to privacy" is a generic term encompassing various rights recognized to be inherent in concept of ordered liberty, and such rights prevent government interference in intimate personal relationship's or activities, freedoms of individual to make fundamental choices involving himself, his family, and his relationship with others.

What is the status of the right to privacy in India? The constitution of India does not explicitly provide for a right to privacy but it was understood that the right to privacy existed as a fundamental right. Recently, the biometric collection by the state under the "Aadhaar Card Scheme" came under attack as being violative of the right to privacy.[24] It was noted therein that the legal position regarding the existence of the fundamental right to privacy was unclear as it was noted that there have been conflicting judgments on the right to privacy and there is a need felt to explicitly decide whether such right is a constitutional right and what are the contours of such a right.[25] The author is of the opinion that the right to privacy should be a fundamental right and ones privacy in the cyberspace can be infringed by many means therefore one must be vigilant and use security tools to protect ones online data.

In terms of infringement by private organizations, players such as Facebook, Google, Marketing Agencies and others have been constantly indulging in the practices of collection of user data[26]. Much of the data shared can essentially be

[17] AIR 1965 SC 881

[18] 413 U.S. 15 (1973)

[19] (2014) 4 SCC 257

[20] See *Devidas Ramachandra Tuljapurkar vs State Of Maharashtra.*

[21] See *Avnish Bajaj vs State*, 2008.

[22] 1970 AIR 1390

[23] Black's Law Dictionary 1195 (6th ed. 1990)

[24] Justice K.S. Puttaswamy (Retd.) & Anr v. Union of India.

[25] Ibid. The matter is currently up for consideration by a larger bench.

[26] http://edition.cnn.com/2012/02/09/opinion/ghitis-google-privacy

treated by them at their discretion.[27] They constantly indulge in something known as data mining[28], which is just one facet of their use of the data. Data mining pertains to corporations collecting data which are stored on their servers and run algorithms to ascertain your likes, potential friends, places you visit often etc. This essentially forms a schematic of one's schedule and life. Though corporations claim transparency, the question as to how the data collected, its extent, use and accessibility is still unanswered. Popular virtual assistants like Siri and Cortana actively collect data to a great extent. Microsoft has recently come into fire for privacy concerns in its latest operating system Windows 10, as the OS collects data by default unless privacy features are turned on.[29] Most persons turn a blind eye or are unaware of the data collection done by corporates. Many are willing to give away their data for perks.[30]

Data once shared, is stored at the will of the organization. This has led to the rise of the recent concept of the "Right to be forgotten".[31] The right to be forgotten leads to allowing individuals to have information, videos or photographs about themselves deleted from certain internet records so that they cannot be found by search engines.[32] This concept has yet to attain popularity in India.

In terms of infringement of privacy by the state, Government surveillance programs are the primary source of such infringement. India has a wide variety of surveillance programs such as Central Monitoring System (CMS), Network Traffic Analysis (NETRA) and National Intelligence Grid (NATGRID). The National Cyber Coordination Centre (NCCC) is one proposed agency which is equated with establishing a system parallel to the PRISM surveillance system of the USA and there is ample concern as to its extent of data collection.[33] There is no clear transparency as to the nature and extent of the data collection that is done by these programs nor is there any clear accountability. Further, most of these programs require compliance on the part of the Internet Service Provider (ISP) and work with them in close tandem.

Section 69 of the Information Technology Act, 2000 imposes an obligation on Internet Service Providers to provide all assistance to government agencies to intercept any communication. In the event of non-compliance, the ISP could be penalized even with criminal liability. Section 66E of IT Act penalizes whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person. Section 5 of The Indian Telegraph Act allows the government to tap phones, though with procedural limitations such as prior permission of the Home Ministry.

It can be very clearly noted that the law relating to the right to privacy is very much in its infancy. Due to recent impetus in technology and its proliferation, these issues have come into light in recent times. A clarification on the right to privacy would be just the beginning in the emergence of the right to privacy in cyberspace in India. Needless to say, state and organizations must be more circumspect in the use and collection of user data and we as private persons should be more aware of our rights and should not turn a blind eye to the issue of our privacy.

D. Crimes related to Cloud Computing

Cloud computing is mistakenly believed to be the Internet with a different nomenclature. Cloud computing is a model to enable convenient and on-demand network access to a shared pool of configurable computing resources like, storage, networking, applications, network, etc. that can be quickly provisioned and released with minimal management effort or interaction with service provider[2]. In other words, it can be said to be a technique to store, having computation power, merge and link infrastructure, business processes and various applications that can be delivered as a service to meet the demands of a client.

The cloud services are being used for criminal activities, they seek to intrude and obtain access to data stored in cloud storage. There exist significant privacy and security issues as well.

According to reports, India has a population of around 8 million businesses which includes small and medium units that are considered as the potential clients of cloud computing services.[34] It is observed and expected that India will attract potential foreign investments in this area. In 2009, the Indian cloud computing market was reported to be estimated at USD 66.7 million (around 33 crores), moreover it was expected to grow at a compounded annual growth rate (CAGR) of 40% over next 5 years.[35]

It raises serious concerns related to cyber-crime and hacking as cloud computing environment and architecture which is not considered secure as a traditional secure network by various specialists. Moreover, complex pitfall of this system is regarding jurisdiction. Since often storage server are located either in foreign jurisdiction or at anonymous location. Simultaneously, investigation is challenge for forensic and law enforcement agencies [8].

IV. Other Cyber-Crimes

There are many other forms of cyber-crimes which are

[27] http://www.digitalstrategyconsulting.com/intelligence/2014/01/facebook_sued_for_data_mining_private_messages.php

[28] http://business.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/

[29] http://thenextweb.com/microsoft/2015/07/29/wind-nos/

[30] http://mashable.com/2014/10/01/data-for-cookies/;http://www.forbes.com/sites/lauraheller/2014/05/01/3375/

[31] http://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/

[32] ttp://www.livemint.com/Industry/5jmbcpuHqO7UwX3IBsiGCM/Right-to-be-forgotten-poses-a-legal-dilemma-in-India.html

[33] http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece

[34] Saurabh Srivastava, Cloud computing is a game changer for Indian businesses, September 2010.

[35] BS reporter, Cloud computing market to CAGR of 40% BusinessStandard, December 2010.

prevalently in the cyberspace. However, some common and intrinsic cyber-crimes will be concisely canvassed in following section.

Hacking: It is the term used when an individual hacks (known as the hacker) a computer system with the intention to break into the system and gain unauthorized access to the data, images and other material placed on the computer. The purpose of such acts is to generally commission frauds, identity theft and other crimes.

One of the earliest report of hacking in India was in March 1999 when Videsh Sanchar Nigam Limited (VSNL) now Tata Communications system was hacked and an e-mail was sent to all subscribers announcing massive cut in internet prices.

Around 38 million accounts were reported to have been breached of Adobe customers by hackers in May 2013, when their source code of Adobe's popular Photoshop program was hacked and parts of the code were stolen. In February 2013 the Twitter account of Burger King was hacked and series of fake tweets floated stating Burger King had been sold out to McDonalds. However, these Tweets gained 5,000 more followers in the first half hour of hacking account thought the Twitter account was pulled down later.[36]

Phishing: It represents fraudulent act in which a Phisher pretends to be from a known and trustworthy company to acquire sensitive information from the target person. In Phishing one is basically tricked into giving their banking details, username, passwords, etc. believing them to be legit imitate. The term phishing originates from the fact that cyber attackers are fishing for data. There exist around four dozen of phishing groups existing worldwide. Various laws address to cyber theft and frauds having different gravity but there are few laws directly dealing with phishing.

Phishing has now been around for more than a decade started with America Online (AOL) back in 1995. About 2 million U.S. citizens' checking accounts[37] were raided by cybercriminal in December 2013.

Vishing- This is a fraudulent technique that employs use of voice over phone systems or the Voice-over Internet Protocol (VoIP) to trick victims and gain access to their personal and financial data. It is one of the forms of identity theft and conducted in two ways. In the first way the victim receives fake email which, appears to be from victims bank or credit card Company instructing the victim to dial a number that intends to confirm bank or credit card details. Second way is when the victim receives call or message to confirm your sensitive personal data to the automated answering machine. In either of the ways the visher gains victim's sensitive and personal data. Moreover, new VoIP services and technology has made it effortless and cheap to gain account details. Also the interactive voice systems sound exactly similar to the systems used by banks and credit card companies.

Key-loggers: They are hardware and software devices which are used to capture strikes on the keyboard. It takes as less as 30 seconds to install key-logger device by which a hacker gets access to entire data and computer processes. Information received can be e-mailed or immediately transfer the data to external controllers. It was initially commissioned by managers for tracking however slowly hackers used them for gaining access to data available on the computer and conducting crimes.

Malware-Viruses: Malware is another term used for viruses introduced in a computer system. Malware is a malicious code planted in the victim's computer machine giving the control to the attacker. Over the years, development of viruses, worms, logic bomb and Trojan horses has become more visible and anyone having basic programming knowledge can construct them.

Virus is a type of malicious code that requires human click to replicate an infected host file like word document. In 1983 computer virus got its formal by Fred Cohen who defined computer virus as 'a program that can infect other programs by modifying them to include a, possible evolved, version of itself'.[38] Once the virus is clicked it executes and the victim really has no way to know that a virus is running. In 1999, *Melissa* and *Papa* viruses made headlines. Melissa is Word 97 and Word 2000 virus spread through an attachment to an e-mail. Similarly, the Papa or Papa.b virus is distributed via excel spreadsheet attached to an e-mail. Virus *Rootkit.Sirefef.Gen* was detected in November 2012 was considered high on damage according to Bitdefender.[39]

Internet Hate Crimes: Every person comes across plenty of offensive material over the internet however not all of it is illegal. Internet is the gate to anonymously generated hate crimes. According to Black's Law Dictionary, Hate crimes are crimes motivated by the victim's race, color, ethnicity religion or national origin.[40]Any material, photo, visual representation, video, audio, content existing on the internet or blogs, chat rooms, emails, social networking sites and others which generate hate crimes based on victims race, color, ethnicity religion or national origin represent hate crimes over the internet.

Spamming: It is the process in which an unsolicited junk e-mail is sent asking people to buy their goods and services from commercial companies. The term 'spamming' originated from a Monty Python[41] skit. These unsolicited commercial e-mails flood the internet with unwanted e-mail that choke or delay e-mails, it clogs internet pipeline. Malware writers make use of spamming techniques to inject viruses, worms, etc.

[36] For more details refer- http://www.mapsofworld.com/around-the-world/recent-hacking-incidents.html.

[37] Current account in a financial bank.

[38] Dr. Frederick B. Cohen, *The Computer Security Encyclopedia Computer Viruses*, http://all.net/books/integ/encyclopedia.html

[39] http://www.bitdefender.com/resourcecenter/virus-encyclopedia/

[40] Black's Law Dictionary, 9th Edn., Thomson Reuters, 2004

[41] British comedy group.

ACKNOWLEDGMENT

This study was financially supported by 'Shree Guru Gobind Singh Tricentenary University' (SGT) University, Gurgaon, Haryana, India. The authors gratefully acknowledge the sponsorship from SGT University, Faculty of Law, Gurgaon, Haryana, India.

REFERENCES

[1] Dr. Amita Verma, *Cyber Crime and Law,* Central Law publication, 1st ed., 2009.
[2] Richard Hill, Laurie Hirsch, Peter Lake, Siavash Moshiri, *Guide to Cloud Computing: Principles and Practice,* Springer Science & Business Media, 2012, pp. 3-9.
[3] Aparna Visanathan, *Cyber Law (Indian & International perspective on key topics including Data Security, E-Commerce, Cloud Computing and Cyber-Crimes,* Lexis Nexis, 2012.
[4] Vakul Sharma, *Information Technology Law and Practice Law & Emerging Technology Cyber Law*ch. 16, ch. 22 &z ch.37.
[5] Michael Simpson, Kent Backman, James Corley, *Hands-on Ethical Hacking and Network Defenses,* Cengage Learning, 2010, pp. 69-71.
[6] Lance James, *Phishing Exposed,* Syngress Publishing, Inc., 2005, pp. 2-11.
[7] *Black's Law Dictionary*, 9th Edn., Thomson Reuters, 2004.
[8] Chirstopher Millard, *Cloud Computing Law*, Oxford, 2013, ch.13.
[9] Scott Mitic, *Stopping Identity Theft,* Nolo, 2009, pp. 100-101.
[10] Ed Skoudis, Lenny Zeltser, *Malware: Fighting Malicious Code*, Prentice Hall Professional, 2004, ch. 1.
[11] Hossein Bidgoli, *Electronic Commerce principles & practice*, Academic Press, 2002.
[12] Dr.Talat Fatima, Cybercrimes, Eastern Book Company, 2011, pp-91
[13] Charandeep Singh Samrao, *Cyber Crimes, Random Publications*, 2013, pp. 22-23.
[14] Dr. Vishwanath Paranjape, *Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India*, Central Law Agency, 2010.

Anchal Mittal . (MBA & LL.M) Born in New Delhi, India on January 28, 1986. She is pursing PhD from Faculty of Law, Delhi University. She received MBA degree from Amity International Business School, Noida, India and in Law LL.M from Guru Gobind Singh Indraprastha University, Dwarka, India. Her area of study in PhD is related to advertising laws.

Yugansh Mittal (BA-LL.B) Born in New Delhi, India on July 18, 1994. He is in the fourth year of the law program me. He is pursing 5 year law program from Vivekananda Institute of Professional Studies, New Delhi, India.