INFORMATION SECURITY
THE VAST ERA OF DIGITALIZATION
With Love

Cyberlekh Publication's
INFORMATION SECURITY

THE VAST ERA OF DIGITALIZATION

March

2019
DEDICATED TO

“Late Dr. A.P.J. Abdul Kalam”

Former President
Republic of India
To all the Readers and Contributors of this book:

Bringing innovative strategies to the attention of policy makers and hence empowering the youth towards the digitalization has always been a highly essential part of the working of “CYBERTALKINDIA”. This book based on the Different papers, is a culmination of different insights which highlight alternative viewpoints, development approaches and innovative technologies backed by analysis and information from various experts across the globe. This book is geared to the needs of practitioners. Through this book, we have tried to bridge the gap between new ideas and theories and field trials.

However, this masterpiece would not have been possible without the valuable contribution from our avid writers. I wish to express my deepest gratitude to all our contributors for their incessant support and for making this entire event a huge success. The authors in this book have harvested to the core problem and have cohesively voiced their opinion in the best possible way.

Kudos to all authors and Netizens!

Mr. Akash Kamal Mishra
Founder & CEO
CYBERTALKINDIA
“An ISO 9001: 2015 Certified and registered Firm in Indore, Madhya Pradesh, India which aims to focus on cybersecurity training and skill development about digital citizenship and internet safety. With the cashless economy boom, there is a pressing need to create a cyber-aware generation.

We have an experience of working over with the School Kids, College Students, Professionals, Law Enforcement Agencies and Senior Citizens on the lines of Cyber Security Awareness. We also offer dedicated courseware on Cyber Security, Cyber Law, and Internet Maturity Education and there are many more things which we offer.

Our founder is one such great personality and has been working day and night for the cyber safety he has completed more over 100+ schools of different cities for the cyber safety awareness and has spoken more than 20k+ students about their safety rights.

CYBERTALKINDIA – Netizens Choice is working day and night for the protection of the Netizens with a positive blessing of the net users available in our country.
We also believe that publication is one such mode to express our views in a different part of the country with this thought we started CYBERLEKH PUBLICATION’S (an imprint of cybertalkindia) our own publication wing to make awareness through our writings and also by the writings of the young Netizens.

We are being recognized by many governments, nonprofit organizations, advocates firms, corporates and also with many educational institutions.

www.cybertalkindia.com
INDEX

• Crimes on Social Networking Sites.................01-10
  ~ Kritika Katoch
• Data Protection & Privacy Concern in Cyberspace11-34
  ~ Ritik Kumar Rath
• Cyber Law in India & Other Countries............35-51
  ~ Tavleen Sood
• Crime Against Women.............................52-59
  ~ Garima Bhaya
• Jurisdiction on Cyberspace.......................60-84
  ~ Toshi Tiwari
• Investigation on Cyberspace.....................85-91
  ~ Amarpreet Kaur Virdi

*****
I

CRIME ON SOCIAL NETWORKING SITES

The internet has the ability to spread or circulate information or communicate instantaneously. This has caused upheaval in many facets of our life. The use of internet in our day to day lives has many disadvantages as now it is used by many people for doing unlawful activities which has further given rise to criminal activities. Latest technologies have enhanced the possibility of invading into the privacy of the individual as the internet is used by many individuals to amass huge amount of private data of an individual, which can be further used for criminal activities.

The Information Technology Act, 2000 on the recommendation of General Assembly Resolution. This act unfolds the various aspects of information technology to promote efficiency in the delivery of government services by means of reliable electronic records.

1.1. Social Networking sites

Social Networking Site is a term used to describe websites which acts as a platform for interaction among people across the globe. It can be in various forms such as forums, blogs
etc. through which people can communicate, exchange ideas and other multimedia.

When a user creates a profile on a particular social networking website, it allows him to share and discuss information and media with either the people on his friend list or with public at large. Social Networking relies upon users building up their own network of contacts on the sites, which in turn introduces them to new contacts. As the user network has increased, the risk related to the privacy of information and media which the user has uploaded has augmented. The crime rate on these networks is accelerating with addition of each user.

1.2. Cyber Crime

Cyber Crime can be explained as any criminal violation or unlawful act taking place on the computer. According to the Information Technology Act, 2000, cyber maybe said to include a computer, computer system or a computer network. Hence, any illegal act which involves a computer, computer system or a computer network s cyber crime. Information Technology Act, 2000 does not explicitly define the term cyber crime. When crime takes place on the Internet there is exchange of information between computers connected to a network where some computers provide
information, some seek for information and there are some which provide for smooth exchanges and route the flow of information.

Computer Crimes can be classified into following categories:

- Conventional Crimes through computer which includes cyber defamation, digital forgery, cyber pornography, cyber pornography, cyber stalking/harassment, internet fraud, financial crimes, online gambling, and sale of illegal articles.
- Crimes committed on computer networks include hacking/unauthorized access, denial of service.
- Crime relating to data alteration/destruction being virus/worms/Torjan horses/logic bomb, theft of internet hours, data diddling, salami attacks, stenography.
- Crimes relating to electronic mail such as spamming/bombing, spoofing.

Cyber crimes familiar to social networking websites are cyber defamation, cyber obscenity pornography, cyber stalking, hacking, privacy infringement, internet fraud, unauthorized disruption of computer system through virus and using any person’s copyright.
1.3. Cyber Defamation
According to Black Law defamation is an international false communication, either published or publicly spoken, that injures another’s reputation or good name. On internet, defamation imputation is published in electronic form. The issues related to defamation on internet include as to time of occurrence, the mode of publication, where the publication took place, i.e. the jurisdiction, who will be liable for the publication of the alleged defamatory statements. Cyber Defamation is covered under section 499 of IPC read with section 4 of IT Act, 2000. Section 499 lays down when the actual defamation takes place while section 4 of the IT Act provides for the legal recognition of electronic records. Therefore if any defamatory information is posted on the internet either through e-mails or chat rooms or chat boards, such posting would be covered under section 499 requirement of publication and would amount to defamation.

1.4. Cyber Obscenity and Pornography
Internet has brought with it vast knowledge and information for the individual and cyber obscenity and pornography is not distant to it. Easy accessibility and wide reach and availability of obscene material on the Internet have made it more convenient for individuals. Cyber pornography refers to stimulating sexual or other erotic behavior over the
Internet which includes pornographic websites, pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, writings, etc. The geographical restrictions no longer exist and therefore, foreign publications can easily enter the local territories in a matter of seconds.

Child pornography on the Internet has been a matter of great concern as they are amongst the biggest users and beneficiaries of the Internet and constitute the most vulnerable group and are the worst sufferers of cyber pornography. Article 9 of the ‘Convention on Cybercrime’ merely imposes a duty upon the parties to offences of producing, offering or making available, distributing or transmitting, procuring or possessing child pornography intentionally and making the offenders criminally liable. Section 67B of the IT Act, 2000 criminalizes all kinds of online child pornography.

1.5. Cyber Stalking

Cyber stalking involves the act to pursue, harass or contact another in an unsolicited fashion using the electronic medium such as the Internet, e-mail, or other electronic communications devices to stalk another person.
Earlier there was no legislation against cyber stalking, but with The Criminal Law (Amendment) Act, 2013 section 354D was added which provided for criminalizing stalking and punishment for committing the offence of stalking.

Cyber stalking may involve electronic sabotage where a cyber-stalker may send hundreds of threatening or harassing e-mail messages by using sophisticated software that sends e-mail messages at regular or random intervals without perpetrator being physically present at the computer terminal.

1.6. Hacking

Hacking is when a computer system is accessed without the express or implied permission of the owner of that computer system. Hacking is usually a pre-planned process, where first a target computer system is identified; it’s security features are studied; tools are developed (passwords and programs) to gain unauthorized access and impair the normal (programmed functioning of a computer or a computer system or computer network. In this kind of crime the computer is a tool as well as the target. It is one of the most popular and fastest rising crimes and has accelerated with the help of Internet.
The meaning and scope of hacking under section 66 of the IT Act, 2000 is beyond than the mere ‘illegal or unauthorized access’ but that should have been done fraudulently and dishonestly.

1.7. Privacy Violation

The internet has many data collection mechanisms which collect a variety of information about surfers like the goods purchased, sites visited, and personal information and so on. It is possible to create profiles on the information collected from a range of sources, which can be paired with information about the user’s computer. The privacy of an individual can be infringed if there is unauthorized access to his account on a social networking website without his knowledge and the person obtains private information without the permission of the person.

There is no direct legislative provision with respect to privacy infringement on the internet but the IT Act, under sections 72 and 72A provides for penalty for breach of confidentiality and privacy and punishment for disclosure of information in breach of lawful contract respectively.
1.8. Internet Fraud

One or more components of the Internet such as chat rooms, e-mail, message boards, or websites are used to refer to any type of fraud scheme. Fraudulent activities can be conducted on social networking websites by persons impersonating to be somebody who they are not in order to commit an offence. Impersonating someone and then taking out information and other personal details also amounts to fraud. One can personally profit at other’s expense if personal information like bank account number, credit card number, telephone calling card number or any other valuable identifying data falls into wrong hands.

1.9. Virus Attacks

Virus attack the computer when programs transmitted are designed in a way to destroy, alter, damage, or even send across data residing in the computer. This transfer can be done by email, or sending messages on social networking websites asking the person to open the link and thereafter the virus attacks the computer system. Section 43 (c) of the IT Act, 2000 lays down the liability to pay compensation to the person who is affected by introduction of any computer contaminant or virus into any computer, computer system or computer network.
1.10. Copyright Infringement

Copyright is protecting original works of authorship that are fixed in any tangible medium of expression. Copyrighted material include the categories of literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphical and sculptural works, motion pictures and audio-visual works, sound recordings, architectural works and computer programmes. Any work copied on the Internet or from the Internet without acknowledging or giving credit to the original author will amount to copyright infringement and the person will be liable of the offence.

1.11. Conclusion

The Internet is a mammoth network of computers and that has made it a boon as well as a bane. On one hand everything has become so easy and convenient from shopping to cooking to playing games etc, on the other hand this has made cyber offenders to take advantage of the situation of this over dependency of people on the Internet. It can be concluded that more stringent laws should be made and implementation of these laws should be the main concern. There is lack of awareness among many individuals using the social networking websites and more often than not they
are hesitant to take action against the offenders committing the offence.
II
DATA PROTECTION AND PRIVACY
CONCERN IN CYBERSPACE

2.1. Introduction

“The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual.”
— Earl Warren

Privacy is generally seen as the ability of a person to maintain some kind of secrecy in his activities which enables him to isolate himself from others in order to protect his interests. And it appears more valuable when you do not have it. When threatened by someone’s faulty action is the time when we understand the importance of security and trust. This can be a consequence of our lives being transformed into data. Every single second of the lives that we live is being stored on the internet as a data and is available to every living soul on the earth. In such a precarious situation what does the word privacy stands for? This question can only be understood by studying the disparate and complex landscape of the internet of things.

1 The fantastic advances in the field of electronic communication constitute, (nov 23, 2018, 10.04 AM), https://www.goodreads.com/quotes/230601
which would further lead us to realization of how to make sure privacy rights are maintained and respected. In today’s world scenario breach of privacy does not occur on a physical level but in the space of internet. This happens because of the mass exposure a person has to this service. Internet when first introduced offered people to transfer their data at high speeds but there was no security vault to keep this data safe, thus disabling the users to control to whom to reveal this data. This disadvantage was ignored by the users due to the compelling nature of the internet and soon more and more individuals and businesses started embracing the power that internet gave us. It was this digitization that required the people to reveal their information. Consequentially protection of online data became important and thus extended the term ‘privacy’ to ‘e- privacy’,

2.2. E- Surveillance- boon or a bane

Our way of interaction in today’s world is affected by the networked nature of digital society. Using online services results in privacy losses that are not always trivial to the users or the regulators. In today’s world social surveillance is not only used to keep a close watch on each other, but also the data of an individual user can be used to infer his private attributes. In an individual perspective, users have the
opportunity to price their personal information and thus the power to balance the benefits, costs, opportunities and risks of online activities. But this perspective is only available if the users are working in isolation. However, the omnipresent nature of internet leaves such a perspective obsolete and can produce results that are unaccounted for to the individual. Users are entering into numerous interactions online being unaware of the fact that large chunks of traces that such interactions are leaving. Such traces are used to know the private attributes of an individual.

An example of a breach of privacy through surveillance is shadow profiles. Shadow profiles are files that contain the private information that they give to use online services. In other cases, these profiles could be made without their permission. In such cases, the person who is being profiled does not submit to terms and conditions of such surveillance.

2.3. Cyber-security

Individual internet users are the pillars of cyber-security. But these often prove to be the weakest link in respect to cyber-attacks. Personal computers are used as the stage of cyber-attacks to spread viruses and malware. Concerns of these

---

computer users are not the greater harm that would be caused to the people at a large scale but they are concerned about their own personal data and thus privacy and rights in general.

2.4. Privacy and Data Protection

Modern practices of privacy focus on no surveillance of communication (communication privacy) and no handling of information about individuals (information privacy).

Information has always been an important tool for the state to exercise control over its population. It is not possible for people to opt out from providing this information. Information technology, such as that used in data mining, aids in collecting data from various govt. sources to conduct analysis and establishing the usual pattern. One of the main issues relating to the collection of data by the government is to maintain a balance between the privacy of individuals and modernization of government function. The government must draw a line so as to restrict itself from using personal data of an individual beyond the necessary government functions relating to public policy. Although in recent years an increase in the appetite of government for collecting personal data for compulsory identification (biometric data) can be seen. Governments authority to collect information,
including a provision for lawful interception of information was broadened by the events of 11 September in the USA and various other legislations in other countries\(^3\). In addition to this EU also has the power to retain data necessary to identify a user for a period of 6 to 24 months.

\textbf{2.5. Edward Snowden Case – citizen data is not secure}

The control that a government holds over the private data of an individual amount to the breach of their privacy. This control came into light by the work of Edward Snowden. On the 20\(^{th}\) May, 2013 a fight started between a superpower and a 30-year-old man just for the sake of privacy. In this Edward Snowden risked his life to bring out the true picture and safeguard the rights of the citizens. This fight ended with showing up the real face of a security agency that in the name of national security they are meddling with individual privacy\(^4\). This fight saw its birth from 1.5 million documents belonging to US secret agency coming before the eyes of individual people making them concerned for their privacy. What acted as a lubricant was the prism program run by the US government for keeping surveillance over its people,

\(^3\) Ibid.

moreover they were not only intruding the privacy of their citizens but also that of all 35 world leaders. In addition, there was a program named XKEYSCORE by which NSA was authorized to monitor everything that you search on the net and that too without consent. NSA to achieve this motive was directly connected to the server of tech companies like Yahoo and Google to procure all the data even those they were not willing to give.

It is not that the US government did not have any reason behind these programs. By the PRISM scheme initiated on September 11, 2001 the government drastically increases the power with the secret agencies using which the intelligence agencies can capture the private data of citizen who are not suspected of any connection to terrorism or any wrongdoing. The tools used by these agencies were evolved after the 9/11 which began under George Bush with the Patriot Act and expanded by the Foreign Intelligence Surveillance Act (FISA) enacted in 2006 and 2007. Also, another initiative of the US government was the XKEYSCORE which is a search engine interface that works by interacting with all the NSA databases for the collected internet traffic, communicated and phone metadata of private citizen. Edward Snowden appreciated NSA’s activities as focused and specifically deployed against legitimate foreign intelligence targets that
the leaders need to protect the security and integrity of the nation. But what he criticized was the use of these tools for surveillance over the citizens of its land. Thus, explaining the XKEYSCORE as legal when used as a part of NSA’s foreign signals intelligence collection system but illegal when used against its own citizens who are not posing any grave threat.

Till now researchers have talked about how government players breach the privacy of individuals but there also are some non-governmental players who play a crucial part in this offense. Some of these players do this for their own benefit for the benefit of others. First researchers would like to talk about those offenders who intrude the privacy of individuals to help the third party gain an unfair advantage over the other. These types of offenders could be easily identified by the study of the case in which a firm allegedly helped establish the government of the largest superpower of the world.

2.6. Cambridge Analytica – And its implications

This issue is related to the US presidential election in 2016 and how Facebook and other company helped Donald

---

5 Ibid.
Trump in winning the election by manipulating data of its user. The main culprit you can say that is not Facebook but Cambridge Analytica which is a British data firm owned partly by Robert Mercer and his family, huge Republican donor of the republic party whose candidate was Donald Trump. The main accusation that they faced was that the organization was drawing flak for its participation in influencing voters’ behavior in the 2016 presidential election. The firm was further alleged to have harvested data of 50 million Facebook users belonging to the US without permission in order to design software to predict and influence people’s voting preference. This data also gave an unfair advantage to Donald Trump’s campaign. But the question that arises is how did Cambridge Analytica gain access to personal data of numerous citizens. This happens when you use an app on Facebook generally a message pop up that the game wants to use your data and people without thinking for a moment, agree to the conditions. The app using this agreement takes data like name, location, number. Even though Facebook says that they share very less data to no data with any third party but Facebook intentionally give

---

some of the data to Cambridge Analytica. In 2014, Dr. Aleksandr Kogan, a psychology professor at Cambridge University, was allegedly paid 800,000 Dollars by CA to develop an app called “THIS IS YOUR DIGITAL LIFE” to take important data of the Facebook users. Although more than 270,000 people downloaded this app and gave their consent to their data being collected, company’s act superseded this consent when they extracted personal information of each of the user’s friends without their consent. Later Kogan passed on all the data collected through his app to Cambridge Analytica and other companies. When people downloaded this app, Kogan not only had access to user’s basic information such as the city of residence and details about friends, but also data firm from the profiles of their Facebook friends. To acquire the full data a certain amount of money was paid to the app users to complete a survey by Kogan’s firm Global Science Research (GSR). This survey also gained permission to access the user’s Facebook account to acquire their personal data. This helped GSR to build personality and psychological profiles of millions of people who were in their radar. The data was allegedly used by Cambridge Analytica to tailor its political advertisement for a group

---

7 Ibid.
individual, whose liking and interest was already known to them. CA used the same strategy in the 2016 US presidential election when the firm worked for Trump. Under the guidance of Brad Parscale, digital director for Trump, Cambridge Analytica performed a variety of service including designing target audience for digital advertisement and fund, modeling voter turnout and determining where trump should travel to best drum up support. On the contrary Facebook deputy general counsel Paul Grewal has endorsed for the falsity of accusations of data breach. He contended that Kogan gained access to information from the users who have signed up for his app and everyone gave consent to the survey. Thus, according to him, no system was infiltrated, and no password or sensitive pieces of information were taken using unfair means. While the perception of various governments is quite different from that of Facebook. One of the examples is the government of UK, which fined Facebook of 500,000 pounds, maximum fine allowed for its role in the Cambridge Analytica case. UK government no longer is concerned with the number of its citizens affected by this scandal (i.e. very less in number) but with the basic right of its citizens to share their information online without a sense of threat in their minds of personal data being stolen that too by one of the largest social networking sites.
Though both the companies are headquartered on foreign lands but that in no way imply that their actions did not have any adverse effects on Indian citizens. We cannot sit at our homes reading of these meddling with an election in some foreign country but we must understand that a critical threat to our digital privacy clouds our country too. This was also reported by Bloomberg, the report stated how Facebook helped the current Indian government on political campaigning and recent reports show that ruling and opposition parties were in contact with Cambridge Analytica. But the question that must come in mind is why the Indian government is silent? This question has a simple answer and that is the long-term relation between Facebook and India. India is the first country to work with Facebook in disaster management and the Indian government does not want to spoil this relation with Facebook. Moreover, Cambridge Analytica on its website claims it worked on Bihar election in 2010 and also that their client achieved a landslide victory. But the reason for this paper is to understand what Cambridge Analytica has that helped them

---

achieve such results? Before presenting their strategies to their clients, Cambridge Analytica using their local knowledge, global reputation, software for political intelligence & election management, access to foremost behavioral change communications methodology in India etc. does caste research, voter demographic analysis, behavioral polling. Based on all such studies company analyses target audience, consult and even does poll planning and management for its clients. Thus, what companies like Cambridge Analytica is not an easy task and that is the reason that they breach the privacy of such a large number of people and charge large amounts for such tasks.

Next in discussion comes those companies who not for the benefit for the other but for their own store and use some personal data of their users. These companies are more dangerous than the companies discussed above because they generally do not conduct any survey or ask for consent but rather keeps a note of all the step taken by an individual on the internet. All these companies to achieve this motive use a software having an innocent and sweet name but is really dangerous as far as privacy is concerned. This term is Cookies.

9 Ibid.
2.7. Cookies- hidden danger to privacy

These technologies are small files on users’ computers or mobile phones that allows the service provider to record information when one visits or interact with websites, application and other tools. This means when one visits or interacts with websites, the third party is authorized to use cookies to make users experience better, for advertising purposes and to improve the website and service. Though these may seem as simple software but they perform various functions like authenticating users on a website, providing requested service, keeping track of information, remembering preferences and using above data to tailor the website to cater to user’s interest. Till now these may seem a really helpful option but the reality is quite different then it seems. In addition to providing better experience cookies can also be used to track people and do things that people may not prefer like delivering targeted ads. Moreover, this is something that has raised reasonable concern among the people. The most important man in the history of cookies is Lou Montulli, who is also responsible for the earliest web developer Lynx in 1991. Later he joined Mosaic Communications Corporation which came to be known as
Netscape in 1994\textsuperscript{10}. Cookies were first used to verify whether users had visited the website before and were a handy solution for e-commerce websites to remember what was one shopping the last time and was shown a pop up add at different websites. To this function, people were not aware until 1996, when media started reporting on the potential threat to privacy. This threat was the concern that the cookies were storing information on the user’s computer without their knowledge or consent. Clearly, cookies make web browsing convenient for us as we don’t have to identify ourselves every time, we visit a website, thus many people don’t see any threat to their privacy because from all its upsides. But unfortunately, the original intent behind the use of cookies has been crushed by some unfair entities who have found a path to use this otherwise harmless process to track one’s movement across the web. These entities are not even stopping after tracking but they move onto using cookies to make detailed profiles of one’s interest, lifestyle. On the face, it might seem harmless and trivial to worry upon by most people, as the worst thing they could do is show targeted ads. But the question is not concerned with the use of one’s personal data rather the concern is the mere fact that

intimate knowledge of one’s preference and private activities might eventually be used to brand each of us as a member of a particular group.

Though unfair use of cookies poses a sufficient privacy threat but it fails to attract attention because of the other major threats like Edward Snowden’s revelations about the NSA and government surveillance. Moreover, cookies are not the main problem but are the equivalent and worst technologies that just happen to caught in mainstream awareness. This is because over 95% of the websites use cookies mostly for unimportant things that would never cross our minds and not all the websites use the cookies in a bad way but only to count visitors and for a quick response. But what has led to the defamation of cookies is its use by large companies like Google and Facebook. These companies hold a vast amount of personally identifiable information like google search may tell about your medical issues and sexual orientation or which political party you support. Sometimes these companies face suits and other times they are just ignored, like in 2012 Google was made to pay $22.5 million as a settlement to over Apple’s Safari Web Browser, where there was a default setting to block third-party cookies that Google bypassed and breached a pivotal law. Certain laws have also seen the light of day against
unfair uses of cookies\textsuperscript{11}. In the USA there have been attempts to introduce legislation like “Do Not Track” law which gives users the right to opt out of being tracked by third party websites. But this was not a success as the difficulty of establishing standards and agreeing workable legislation seems to have retarded its progress. European Union was the organization acknowledge the grave threat imposed by misuse of cookies and thus introduces a certain set of rules.

2.8. EU cookie law\textsuperscript{12} - prevention from threat

The law was changed in May 2011 by the e – privacy directive with regard to cookies in the European Union. According to the new law, website owners were charged with telling visitors about the cookies they use and obtaining their consent. Complying websites now show a pop up when one first visits the link, explaining their cookie policy and allows individual to accept it. In the latest study by ICO, which reveals that on an average website places 34 cookies on your device on your first visit, and 70 percent of them are known as third-party cookies (set by other websites other than the one being visited).

\textsuperscript{11} Ibid.
\textsuperscript{12} EU Cookie Directive . (2009)
Moving onto the next part of the document that deals with breach of privacy by an individual of another individual. This kind of breach is one of the most dangerous ones due to the difficulty of keeping an eye on each and every individual. One of the most prevalent examples for this kind breach could be Revenge Porn. This is one of the less talked off topics but includes all the essentials of publication of personal data without consent. Further, the researchers would like to elaborate on revenge porn as an act done without consent.

It was in 1964, when a famous line was said by American judge Potter Stewart famously said “I can't define pornography, but I know it when I see it.” The reverberations of these words can be felt across the globe even after fifty years. It is known that one man’s art is another woman’s erotica is another person’s sex tape. In today’s world the internet has turned into an intrepid, empathetic and nuanced account of the sexual shopping cart, thus ‘Revenge’ helps in limiting the scope of this offense to inducement through personal vengeance, whereas such an act could be motivated by a desire for profit, notoriety or no reason at all. All images of nudity are intrinsically

13 Jacobellis v. Ohio, 378 U.S.184 (1964)
pornographic and this can be impliedly derived from the term ‘porn’. Following this definition, sexually explicit images created and shared within the bounds of a private relationship should not be considered pornographic unless and until they leave the 4 corners of personal relation to being converted into public sexual entertainment. The history of publishing obscene personal images without the consent could be traced back to 1980s when a magazine named hustler which featured image of naked girl called ‘beaver hunt’ but the problem with this section was that not all the woman gave their image with consent and they published such images without verifying information on forged consent forms. Revenge porn got its major attention in the year 2012 when Hunter Moore launched a website ‘is anyone up’ that was a user- submitted pornography site. Moreover, this site contained personal information of the victim and this was also a threat to the personal life of the individual. A person by the name of Charlotte Laws was the first person to criticize this but the fans of this site sent her death threat. At that time there were no established principles for an individual’s privacy thus there was no sense of guilt among the fans of this site for they were destroying someone’s life. This impliedly means that the concept of consent of the victim was considered as non- existent.
2.9. Revenge porn in India – danger to the reputation of a person

India is the 3rd largest country in term of porn video viewership in the year 2017, and the growth of porn viewership rose by 121% in 2017 only. The main reason is the proliferation of smartphone in 2013 as it was close to 44 million but now it is more than 337 million. Revenge porn is defined in Oxford dictionary as “Revealing sexually explicit images or videos of a person posted on the Internet, typically by a former sexual partner or any other person, without the consent of the subject and in order to cause them distress or embarrassment and degrade the reputation of the subject” \(^{14}\). Most popular case in India was the DPS MMS clip. The DPS MMS resulted in arising of amateur videos, it becomes a flood gate in India of revenge porn videos and the number of videos was shared across the internet. What happens with victim of revenge porn is that they suffer in many ways when clips are leaked and distributed, it forces people to changes their names, identity, and sometimes even their physical attributes. And even if the video is filmed and as always women face the brunt of it. The occurrence of these kind of cases led to multiple platforms in 2015, Facebook, Twitter

and reddit, announced banning of revenge porn on their websites. The essential element of revenge porn is that the perpetrator and the victim shared an intimate relationship and that the former has deliberately (and without the victim’s consent) released sexually explicit information of the subject online in order to cause distress and harm to the victim's reputation. While revenge porn and non-consensual porn are used interchangeably, there is a noticeable difference between them. Non-consensual porn includes within its ambit sexually explicit images captured without a person’s knowledge or consent. But in the case of revenge porn, it is very different as it often includes such sensitive information that was voluntarily been captured or send to the perpetrator in good faith in the course of an intimate relationship that should not have been made public. But later released by the person with whom the act was done or with the interference of a 3rd party. In such a precarious situation what is important is to analyze the number of victims and make the subsequent laws to prevent such act of breach. Although in the national crime record bureau’s document on cybercrime against women, there is no official statistics available that pertains specifically to revenge porn in India. A 2010 report suggests that “only 35 percent of the women have reported about their victimization.
46.7% have not reported it and 18.3% have not been aware of the fact that they have been victimized. The recent situation of revenge porn has prompted various countries to enact legislation that criminalizes it. Some of these countries include the UK, Canada, Australia, Japan and the Philippines.

In India, nonconsensual distribution of images captured with consent is dealt with by the section 354C\textsuperscript{15} of the IPC. However, this section has limited its scope to female victims and male offenders, not vice versa.

Transmission of images depicting the private areas of a person is punishable under section 66E\textsuperscript{16} of the IT act. The Explanation to the section limits only to private area to “…the naked or undergarment clad genitals, pubic area, buttocks or female breast”. This provision is gender-neutral and captures every aspect of revenge porn and not even addressing it by name. However, the narrow definition of “private areas” in this case could limit the applicability of the act in this type of cases where the victim is captured in

\textsuperscript{15} Indian Penal code , sec 354(c), 1860
\textsuperscript{16} Information Technology Act , sec 66(e), 2000
an intimate position without showing those particular areas this act will not be applicable 17.

Section 67A18 of the IT Act punishes the offender who made publication or transmission of “material containing sexually explicit acts, etc. in electronic form”. While this can punish perpetrators effectively, it also contains risks including within its ambit, victims who may have voluntarily captured and shared such private content with their partners19.

In the case of JPH v. XYZ & Ors20 which is a landmark case in which JPH has been in a relationship with XYZ for a number of months, during the course of which a number of pictures and videos were taken by JPH which showed nudity and sexual activity 21. XYZ sent a series of communications to JPH threatening to post the images on social media and/or to cause them to be published in magazines the court granted an interim non-disclosure order restraining the disclosure or publication of images and information in a so-called "revenge porn" case.

17 Supra 13
18 Information Technology Act, sec 67(a),2000
20 JPH v. XYZ & Ors [2015]EWHC 2871(QB)
21 Supra 13
And this was further proven in the case of MM v. BC, RS and Facebook Ireland Ltd\textsuperscript{22}. In this case the plaintiff alleged that she has been the victim of revenge porn. She states that she sent, either one or more, highly sexualized photographs of herself to one of the defendants, at a time when they were in a relationship. That subsequently, after the relationship came to an end, one of those photographs was published by the defendants. She asserts that this undermined her independence, her dignity, her right to privacy and was in breach of the Data Protection Act 1998. Here court said revenge porn victim should be helped to live a life of free from harassment, abuse and instances of revenge porn.

2.10. Conclusion

During the duration of this research, the researchers analyzed different ways in which the personal privacy of an individual can be and is breached. These ways include both government and non-government actors. Though breach of privacy by government actors attracts more of attention as compared to that of non-government actor but that in no way implies that breach of privacy committed by individuals is less dangerous to the society and its citizens. With the advancement of technology and widespread use of internet,

\textsuperscript{22} MM v. BC, RS and Facebook Ireland Ltd NIQB 127 [2017]
on one side people are being benefited and on the other side, they are some players using every opportunity they get to exploit the personal information of these people. Government though treated as the savior of a nation and its peace, in this modern world has been accused of breaching the privacy of its citizens. There is very little left to trust upon in the world of internet of things. With the study of concept of revenge porn, researchers explained how the ones we loved become the predators of our privacy and threaten not only our dignity but also our mere existence with liberty. In such situations come up the people who act in favor of the people by disclosing the wrongful acts of the offenders by shedding some light on the truth. But the case finally rests with the government who themselves have used unfair means to come in power. These unfair means include all the acts ranging from keeping surveillance over its own people to befooling them or inducing them through targeted advertisements regarding their campaign.

*****
III

CYBER LAW IN INDIA & OTHER COUNTRIES

As we all know that this is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. Since the web is considered as worldwide stage, anyone can access the resources of the internet from anywhere. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current status to determine whether they are sufficient to combat the kinds of crimes discussed in this report. Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes. In order to stop or to punish the cyber criminals the term “Cyber Law” was introduced. We can define cyber law as it is the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, encompassing many subtopics as well as
freedom of expressions, access to and utilization of the Internet, and online security or online privacy. Generically, it is alluded as the law of the web.

3.1. Introduction to cyber law in India and other countries

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other’s benefit since decades. This gave birth to “Cyber Crime”. It doesn’t have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law. The UN’s General Assembly recommended the first IT Act of India which was based on the “United Nations Model Law on Electronic Commerce” (UNCITRAL) Model. Cyber crimes are unlawful acts where the computer is used either as a tool or
a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber-crime. These crimes are discussed in detail further in this chapter. A comprehensive discussion on the Indian law relating to cyber crimes and digital evidence is provided in the ASCL publication titled “Cyber Crimes & Digital Evidence – Indian Perspective. The most common cyber-crimes are cyber thefts which also includes identity thefts, fraud, forgery, defamation, pornography and hacking. Reports show that forgery was done mostly by youngsters in the age group of 18-30 years, whereas cyber frauds were committed mostly by middle aged people in the age group of 30-45 years.

3.2. **Aim & objectives of cyber law in India and other countries**

When more and more people are using the digital format whether in the form of mobile phones as also communication devices and computers, it is but natural to expect that they would be facing large number of cutting-edge legal issues in cyberspace.
The aims and objectives of the Cyber law are as follows:-

- To create more awareness about cyber legal issues and challenges
- To provide advice, inputs as also guidance to people on their day-to-day legal issues concerning the use of cyberspace
- To work on research and development on cutting-edge issues and challenges in cyberspace
- To contribute to the global debate on evolving Cyber Law jurisprudence
- Dedicated encryption laws need to be formulated.
- The concept of Cloud computing should be given a legal acceptance.
- E-mail policy has to be formulated and implemented.
- Legal issues of online payments
- The legal aspects of online gambling and online pharmacies need to be reconsidered.
- The legal aspects of Bitcoins need to be reconsidered.
- Framework for blocking websites
- Regulation of mobile applications
3.3. What is the need and importance of cyber law and security?

Cyber Law deals with the legal issues of the internet usage and all devices connected over the network, their proper use in order to prevent and control cyber crimes. Since the internet is all over the world the rules and regulations are a bit cloudy but we need to keep in mind a few things to ensure that we are using the internet in a proper and safe manner without causing any trouble.

1. The internet's jurisdictional boundaries may not be clear but the users are bound by the jurisdictional laws of the area in which they reside.

2. Do not access web sites that may not be approved by the jurisdiction in your area.

3. Do not post any offensive material that may cause an outrage among other internet users. Articles with an offensive tone on sensitive subjects like religion, politics etc., Uploading child pornography and other offensive materials is considered a crime in many countries and is punishable depending upon the country's laws.

4. Illegally downloading and distributing protected items like intellectual property and copyrighted articles is a cyber crime and those who are caught engaging in such acts can be prosecuted.
5. Duplication of content or software from CDs and DVDs that are copyrighted and distribution of these on the internet is punishable.

6. Stealing user information (phishing) and impersonating a user (ID theft) are serious cyber-crimes.

7. Sending bulk messages that can affect networks and jam mailboxes is called spamming. The US introduced CAN-SPAM Act in 2003 that allows prosecution of spammers.

8. Illegal bank transactions through internet, to any dangerous individuals who might threaten national security is a cyber-crime that will be considered as a breach of national security and those caught engaging in such acts can be punished by the government.

Even though the Cyber Laws are not very clear to everyone the increase in cyber-crime rate has pushed many governments to introduce Acts that would govern the cyber space at least within their jurisdictions. The governments of USA, UK, Canada and China have enforced Cyber Laws to control Cyber-crimes. The other nations that have followed in introducing Cyber laws are India, Australia, Malaysia, Iran, Iraq, Indonesia, Thailand etc. Among all these nations China emerges to be the strictest in its laws regarding the use of the internet.
3.4. History of cyber law in India

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information. The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft. After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill.
However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber crime and to facilitate speedy locating of a cyber criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. Finally, this suggestion was dropped by the IT Ministry in its final draft. The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.
3.5. Information Technology Act 2000

Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cyber crimes and liability of network service providers.

The Preamble to the Act states that it aims at providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and aims at facilitating electronic filing of documents with the Government agencies.

This Act was amended by Information Technology Amendment Bill, 2008 which was passed in Lok Sabha on 22nd December, 2008 and in Rajya Sabha on 23rd December, 2008. It received the assent of the President on 5th February 2009 and was notified with effect from 27/10/2009.

The IT Act of 2000 was developed to promote the IT
industry, regulate ecommerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules. [ Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008].

3.6. Information Technology Act Amendment 2008

The term 'digital signature' has been replaced with 'electronic signature' to make the Act more technology neutral.

i. A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.

ii. A new section 10A has been inserted to the effect that contracts concluded electronically shall not be
deemed to be unenforceable solely on the ground that electronic form or means was used.

iii. The damages of Rs. One Crore prescribed under section 43 of the earlier Act of 2000 for damage to computer, computer system etc. has been deleted and the relevant parts of the section have been substituted by the words, 'he shall be liable to pay damages by way of compensation to the person so affected'

iv. 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates

v. Sections 66A to 66F has been added to Section 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.

vi. Section 67 of the IT Act, 2000 has been amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Rs.100,000 to Rs. 500,000. Sections 67A to 67C have also been inserted. While Sections 67A and B deals with penal provisions in respect of
offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

vii. In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, sections 69A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

viii. Section 79 of the Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if;
ix. A proviso has been added to Section 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

3.7. Present Scenario

India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security. According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014. In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011. As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively. There has been an annual
increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years.

3.8. Case Laws

1. Pune Citibank Mphasis Call Center Fraud

Some ex-employees of BPO arm of Mphasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection". The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust" etc are therefore applicable in the above case in addition to section in ITA-2000. Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damage to
the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2. The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

3. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go
undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

3.9. Conclusion

The rise and proliferation of newly developed technologies begin start to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cyber-crimes. The Act further revise the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891 and the Reserve Bank of India Act, 1934. Any part of the world cyber-crime could be originated passing national boundaries over the internet creating both technical and legal complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and cooperation among various nations are required to take action towards the cyber-crimes. Our main purpose of writing this paper is to spread the content of cyber-crime among the
common people. At the end of this paper “A brief study on Cyber Crime and Cyber Law’s of India” we want to say cyber-crimes can never be acknowledged. If anyone falls in the prey of cyber-attack, please come forward and register a case in your nearest police station. If the criminals won’t get punishment for their deed, they will never stop.

*****
IV

CYBER CRIME AGAINST WOMEN

Internet has redefined the virtual life of ordinary individuals and has given a wide variety of opportunity to its users including women. It has given a platform to its users where they can exchange ideas, communicate with like-minded people and participate in the development of virtual societies as per their choices.

Social networking websites is one of the most popular segments of internet amongst its users. However there is a dark side to social networking websites too, it has become a sanctum for cyber criminals to victimize women, a peril target on the web, after children.

Even in today’s modern world women are treated inferior to men in various spheres of the society which in turn creates a huge gender bias between men and women where the men think that even their wrong acts towards the women shall not be penalised. Cybercrime works in a similar manner where the internet offenders are not afraid of any authority which can punish them.

The world of internet has a virtual reality or even hide his true identity, this gift of web is used by the criminally
minded to commit wrong acts and then hide under the blanket provided by the web.

4.1. What is Cybercrime?

‘Cybercrime’ is the term used for any illegal activity that uses a computer as its primary mode of commission. An offence that is committed against individuals or group of individuals with the criminal basis of harming either the reputation or any causing physical or mental harm to victim directly or indirectly, using modern telecommunication networks such as Web.

Women especially young girls inexperienced or who have been newly introduced to the world of web and fail to understand the vices of internet are considered as a vulnerable target, falling into the bait of cybercriminals and bullies.
- **Cyber Harassment**

The use of email, derogatory websites and instant messaging or otherwise harass an individual or group through personal attacks shall be defined as Cyber Harassment. This can be in the form of flames, sending offensive or cruel emails, harassing others by posting on blogs or social networking websites or otherwise harass an individual or group through personal attacks.

Cyber harassment is difficult to track as the person responsible for the acts of cyber harassment remains anonymous while threatening others online. This usually applies to school age children.

- **Cyber Stalking**

Basically the behaviour of the offender wherein he or she wilfully and repeatedly engages in a knowing course of harassment directed at another person reasonably or seriously alarming or terrorizing that person.

This is one of the most popular crimes of the web world.
This usually occurs with women who are stalked by men, or children who are stalked by adult predators or paedophiles. Cyber stalkers harass the victims through open publishing websites, discussion forums, websites and chat rooms.

The motivation of cyber stalkers can be considered less than 4 reasons:–

   a) Sexual Harassment
   b) Ego and power trips
   c) Obsession for love
   d) Revenge and hate

4.2.Ritu Kohli Case

This was the first case of cyber stalking in India.

In this case, Mrs. Ritu Kohli filed a complaint in the police station against a person who used her identity to chat over the web mostly in and around Delhi for four consecutive days. She further complained that the person was chatting on the internet using her name and giving her address and even used obscene language. Moreover, that same person was also deliberately giving her phone number to the chatters and encouraged them to call her at odd hours.

Consequently, Ritu received 40 calls within the span of 3 days that too at odd hours. These calls created a mayhem in the complainant’s personal life.

The offender’s IP address was traced, investigation was done by the police and the cybercriminal was arrested. A case was

23

registered under section 509 of IPC but later on the offender was released on bail.

Similar to the case of Email Harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered under the ambit of section 72 of the IT Act that the cyber criminal can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under section 441 of IPC for criminal trespass and section 509 of IPC for outraging the modesty of a women.

- **Cyber Pornography**

  It simply refers to the portrayal of sexual content on the internet. This is another threat to the female netizens as they never know which action of theirs is being recorded and would later on end up on the web.

  The **DPS MMS scandal** ²⁴ is a very famous case of cyber pornography where an MMS clip a school girl in compromising situation was made and distributed amongst the netizens.

  Unlike other cybercrimes, Cyber Pornography is an exceptional case which has been covered in section 67 of the IT Act 2000.

  Another example of cyber pornography would be the recent case of **Delhi Metro CCTV Footage Leaks** ²⁵. In this case the CCTV recording of couples getting intimate at metro stations which was recorded by the police security cameras was leaked on the internet.

• Cyber defamation

This kind of a situation arises when defamation takes place with the help of computers and/or the web.

SMC Pneumatics (India) Pvt. Ltd. Vs Jogesh Kwatra\textsuperscript{26}

In this case cyber defamation was reported when a company’s employee (the defendant) started sending defamatory, derogatory and obscene email’s about its managing director. The emails were anonymous and frequent and were sent to many of their business associates in order to tarnish the goodwill and image of the firm (Plaintiff). The plaintiffs could identify the offender with the help of a computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the defendant from sending emails which are obscene, derogatory or defamatory to the plaintiffs.

This was the very first instance of cyber defamation in India which was recorded.

The State of Tamil Nadu vs Suhas Katti\textsuperscript{27} – this was the case wherein a lady had to go through cyber defamation. Here obscene and defamatory messages were posted about a divorcée women on the yahoo message group. Moreover, emails were also forwarded to the injured party by the offender with the help of a false email id created by him in the name of the victim (injured party). The incidence of posting the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

\textsuperscript{26} http://www.legalserviceindia.com/lawforum/index.php?topic=2240.0
\textsuperscript{27} http://lawmantra.co.in/tamil-nadu-v-suhas-katti-2004-case-related-to-the-posting-of-obscene-messages-on-the-internet/
Morphing

It refers to the situation wherein the picture is edited up to a great extent that it looks completely different from the original one. In such cases what happens is that the cyber criminals download photograph of girls from the social networking site and then morph it with another picture in which the girl is in a compromising situation, so as to indicate that the girl whose picture was initially taken from social networking site indulged in such activities.

After all this the cybercriminal then starts blackmailing the victim of releasing those morphed pictures.

Such acts can be penalised under the IT Act. The offender can also be booked under IPC.

Email spoofing

This refers to a situation wherein the email though by details show something else whereas in reality the email actually originated from some other source. This method is often used to extract personal information from the users and private images from unsuspecting ladies and later on these images are used to blackmail those ladies.

4.3. Reasons for growth of cybercrime against women in India

Many a times the cyber-crime goes unreported simply because the women feel shy and are scared of the stigma that might get attached and also the fear of defamation against her family. In many cases women start blaming themselves for the crime done to them.
Women are more vulnerable since they remain scared because of not knowing the identity of the offender and also because the fear that build up in them because of being blackmailed by the cybercriminal.

Moreover, women fear that if they get up and speak for themselves they might not get the amount of support they expect to be getting from their family members and also under the fear that what impression would the society form for them.

It is because of these fears that women do not get crime reported which results in giving these offenders high spirits to commit more such crime.

4.4. What victims need to do?

Even after so much of modernisation women still fear getting such an incident of cybercrime reported and also the police doesn’t take it much seriously. In such case victims should straight away contact the women assistance cell or an NGO which will guide them through the process and also will make sure that police does not take the case lightly.

*****
V

JURISDICTION IN CYBERSPACE

5.1. Introduction

With the advent of the Internet, cyber law has become an emerging field. Cyber law encompasses cyber-crime, electronic commerce, freedom of expression, intellectual property rights, jurisdiction and choice of law, and privacy rights. Cyber crime involves activities like credit card fraud, unauthorized access to computer systems, child pornography, software piracy and cyber stalking. Electronic commerce includes with encryption and data security. Freedom of expression includes defamation, obscenity issues and censorship. Intellectual property rights cover copyright, software licensing and trademark protection. Jurisdiction focuses on who makes and enforces the rules governing cyberspace. Privacy rights addresses data protection and privacy on the Internet.

There are many issues to be resolved in Cyber law. Two areas of cyber law requiring further clarification are cyber crime and jurisdiction. For example, in cyber law there are only a limited number of cases on point and no major statutory schemes on the books. Policy makers and attorneys dealing with cyber crime are often confined to referring to the imprecisely applicable and scarce existing statutes and cases.\(^28\)

In cyber jurisdiction, the Court must address the question of which lawmaker has jurisdiction over actions taking place on the Internet. In the few cases the Courts have adjudicated,

they have applied long-arms statutes and personal jurisdictional principles in making decision. Due to the paucity of cyber jurisdiction cases, there is a limited amount of law for the legal practitioner for reference.

5.2. Cyber Threats

The FBI defines a cyber incident as “a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks” (2017). While data breaches can happen in many ways, this article focuses on the potential for targeted attacks.

Four types of cyberattacks are particularly concerning for state courts.

1. **Phishing** uses social engineering to solicit personal information from unsuspecting users to compromise their own systems. Phishing e-mails appear legitimate and manipulate users to enter items, such as usernames or passwords, that can be used to compromise accounts. Spearphishing, a more personalized method, could target specific judges and court employees.

2. **Ransomware** infects software and locks an organization’s access to their data until a ransom is paid. Through phishing e-mails, drive-by downloading, and unpatched software vulnerabilities, cybercriminals attempt to extort users by encrypting their data until certain conditions are met. The result is a temporary or even permanent loss of data.

3. **Advanced persistent threat (APT)** attacks attempt to maintain ongoing, extended access to a network by
continually rewriting malicious code and using sophisticated evasion techniques. A successful APT attack results in complete invisible control of systems over a lengthy period time. APTs typically use socially engineered attacks to get a foot in the network door.

4. **Code-injection attacks** involve the submission of incorrect code into a vulnerable computer program without detection. Through these attacks, cybercriminals trick the target system into executing a command or allowing access to unauthorized data. The most common code injection attack uses Standard Query Language (SQL) through an online application.

5.3. **Cyber security**

In our hyper-connected world, the technology that we rely on also makes us more vulnerable. State court systems are no exception. The many benefits of technology are accompanied by risks and challenges. Unfortunately, cyberattacks on individuals and organizations continue to rise in frequency and sophistication. The Federal Bureau of Investigation (2017) reported that cyberattacks in the United States caused over $1.3 billion in victim losses during 2016. Generally, cybersecurity involves the protection of computers and information systems from theft, damage, or disruption. More specifically, Craigen, Diakun-Thibault, and Purse (2014) define cybersecurity as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from...
occurrences that misalign de jure from de facto property rights.”

5.4. Cyber Jurisdiction

The term “jurisdiction” refers to the authority of a court to hear a case to resolve the dispute. In other words, court’s power to decide a case or issue a decree depends upon its jurisdiction. Since the legal environment of e-commerce has no geographical boundaries, cyber jurisdiction extends to all communications to anyone who has access to website.

The law of cyber jurisdiction involves determination whether a particular activity in cyberspace is controlled by the laws of the State or country where website is located, or by the laws of the State where Internet Service Provider (ISP) is located, or by the laws of the State where user is located or by all these law?

The Internet can be seen as multi-jurisdictional because of the ease which a user can access a Web site anywhere in the world. It can even be viewed as a-jurisdictional in the sense that from the user’s perspective state and national borders are essentially transparent.

For courts determining jurisdiction, however, this situation is more problematic. The court in Zippo Manufacturing Co. v. Zippo Dot Com Inc. said there is a global revolution looming on the horizon, and the development of the law in

29 https://www.ncsc.org/~/media/Microsites/Files/Trends%202018/Cyber security-Protecting-Court-Data-Assets.ashx
dealing with allowable scope of personal jurisdiction based on Internet use is in its infancy.

The developing law of jurisdiction must address whether a particular event in Cyberspace is controlled by the laws of the state of country where the Website is located, by the laws of the state or country where the Internet service provider is located, by the laws of the state or country where the user is located, or perhaps by all of these laws.\(^3\)

Cyber jurisdiction issues have been dealt with primarily in the civil courts. Since the advent of U.S. v. Thomas,\(^3\) and Minnesota v. Granite Gate Resorts Inc,\(^3\), however, cyber jurisdiction issues have begun to be examined in criminal courts as well.

### 5.5. Targeting Courts

State court systems are guardians of sensitive data for individuals and organizations. Court records are crucial in the functioning of our society. Preserving these official records is a responsibility long held by judicial-branch administrators. The Judiciary Act of 1789 created the first position of district court clerk to record deeds and judgments of the courts (Sec. 7). Much has changed in the nearly 229 years since. Today, modern court administrators have extensive data-governance responsibility. Data governance includes the people, processes, and technology required to properly handle an organization’s data assets. Included under this umbrella are data quality, usability, integrity,

---

\(^ {33} \) Stuart Biegel, supra note 9, at 2  
\(^ {34} \) 74 F. 3d 701 (6th Cir. 1996) (USA)  
\(^ {35} \) 568 N.W. 2d 715 (Minn. App. 1997); aff’d 576 N.W. 2d 747 (Minn. 1998)
security, and preservation. Data governance truly touches all aspects of a court organization.

The landscape of court technology has changed rapidly, as digital tools help facilitate the business process of the court. This proliferation of technology has improved the judiciary’s access and transparency, while also significantly increasing data storage and the digital footprint. Consequently, there are multiple entry points for data breaches in the judicial branch. These include judiciary case management systems, networks, servers, cloud storage, software programs, Wi-Fi systems, employee devices, and an array of court-specific technology. No longer is just one desktop PC assigned to each employee within a court facility. Judges and court staff now use laptops, tablets, and smart phones to conduct court business. These devices are used outside the confines of the courthouse, accessing networks within and across jurisdictional lines.

5.6. Responding to Cyber attacks

Even with the best of intentions and diligent preventative measures, data breaches happen. A cyber-incident response team should be created in the planning process. Immediate, strategic action on the part of the victimized organization is required to minimize damage and expedite recovery. Essential first steps for courts include pinpointing the area of intrusion, minimizing exposure and attack surface, and understanding the scope of the attack. For example: Was just a family-court case management system compromised? Was the breach confined to only certain courts in the state? Data on all attack-related events must be collected and logged, as it will be vital in the attack investigation. After a breach is discovered, the attack should be reported to at least one law-enforcement agency. Within the federal executive branch,
the United States Department of Justice, Department of Homeland Security (DHS), and FBI provide guidelines and best practices for responding to cyber attack incidents. These agencies supply secure forms to report cyber incidents for analysis. The Multi-State Information Sharing and Analysis Center (MS-ISAC), created by DHS, is the key resource for cyber-threat prevention, protection, response, and recovery for state and local governments. MS-ISAC is a voluntary and collaborative effort that serves as a central resource for situational awareness and incident response for state and local governments. Membership is open to all state and local governments at no cost. The Washington State AOC collaborated with MS-ISAC to determine the scope of their 2013 data breach. In addition to data-asset threats, shutting down court systems because of a cyber attack can have massive operational impact on normal court business. In these instances, courts must be able to hold time-sensitive and constitutionally mandated hearings, as well as issue warrants and orders. Courts also have to consider filing access for those parties bound by a filing statute of limitations. When necessary, impacted jurisdictions can issue an order tolling case activity during operational disruption. Sharing timely and accurate information to all impacted by the breach is crucial. Once the type of attack is identified and understood, sharing this information with other court systems is beneficial. Creating a heightened awareness for specific attacks, along with actionable information, provides great value to the court community.

1. Cyber Jurisdiction In Civil Cases

In determining whether jurisdiction exists over a defendant, the U.S. Federal courts apply the law of the forum state,
subject to the limits of the Due Process Clause of the Fourteenth Amendment.\textsuperscript{36}

In Inset Systems, Inc. v. Instruction Set, Inc.\textsuperscript{37} the court held that advertising over the internet was purposefully directed toward the forum state.

The US District Court for the Eastern District of Missouri reached a similar conclusion in Martiz, Inc. v. Cyber Gold, Inc.\textsuperscript{38} finding that it had jurisdiction over a California defendant in a trademark infringement case, where the defendant’s only contact with the state was through its California based website, which was accessible in Missouri.

In McDonough v. Fallon McElligott, \textsuperscript{39}the court dismissed plaintiff’s contention stating that—because the web enables easy worldwide access, allowing computer interaction via the web to supply sufficient contact to establish jurisdiction would eviscerate the personal jurisdiction requirement as it exists. Thus, the fact that defendant has a web site used by Californians cannot establish jurisdiction by itself\textsuperscript{40}.

Similar decision is Pres-Kap, Inc v. System one, Direct Access, Inc.\textsuperscript{41} which involved electronic contacts through a computerized airline reservation system. In Burger King Corp. v. Rudezuitiz\textsuperscript{42} the US Supreme Court asserted jurisdiction on the grounds of accessibility of Internet. The court asserted that when a defendant has purposefully directed its activities to a forum state and caused injury to an

\begin{itemize}
  \item \textsuperscript{36} U.S.C. Const. Amendment. XIV
  \item \textsuperscript{37} 937 F. Supp. 161 (D. Conn. 1996)
  \item \textsuperscript{38} No. 96-CV01340 (E.D. Mo. Aug. 19, 1996)
  \item \textsuperscript{39} No. 95 Cir 4037 (S.D. Ca. August 15, 1996)
  \item \textsuperscript{40} Supra note 14
  \item \textsuperscript{41} 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994)
  \item \textsuperscript{42} 471US 462 (1985)
\end{itemize}
individual or entity, the state’s invocation of jurisdiction comports with its Due Process obligations.

2. Cyber Jurisdiction In Criminal Cases

The question of cyber jurisdiction in a criminal case came to the forefront of attention in early 1996 in U.S. v. Thomas when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. The defendants began operating the Amateur Action Computer Bulletin Board System (AABBS) from their home in Milpitas, California in February 1991. The AABBS contained approximately 14,000 Graphic Interchange Format (GIF) files. These files could be accessed by members who possessed the password. Once the password was entered, the users were able to select, retrieve, or download the GIF files to their own computers.

The government got involved in AABBS activities when a Web surfer found the site, explored the introductory screens, was offended and subsequently complained. In 1994, a U.S. Magistrate judge for the Northern District of California issued a search warrant authorizing a search of the defendant’s home. Because of the evidence found their computer system was confiscated.

---

44 74 F.3d 701 (6th Cir. 1996)
The defendants were convicted in the U.S. District Court, Western District 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 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 defendant asserted that the GIF files were an intangible string of 0’s and 1’s, which only became viewable images after being decoded in the AABBS member’s computer. The court disagreed, ruling that the fashion in which the images were transmitted did not affect their ability to be viewed or printed out by members in Tennessee. The defendant also argued that they were prosecuted under the wrong statute and that their conduct, if criminal at all, fell within the prohibitions of the statute which addresses commercial dial-a-porn operations. The court declined to accept this argument. Instead, it ruled that the statute must be construed to affect the intent of Congress, which was to prevent the channels of interstate commerce from being used to disseminate any obscene matter.

3. Cyber Jurisdiction In International Cases

When adjudicating cases involving 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 interest

of the federal government in its foreign relation policies. When extending jurisdiction into the international field great care and reserve must be exercised.\textsuperscript{46}

Because of these sovereignty concerns, there is a higher jurisdictional barrier when litigating against The Supreme Court in Asahi Metal Industry Company v. Superior Court,\textsuperscript{47} indicates that a plaintiff seeking to have a foreign citizen into court in the United States must meet a higher jurisdictional threshold than is required when the defendant is a United States\' citizen. In Asahi the court found that even though Asahi had minimum contacts with the forum state, it would be unreasonable and unfair to find jurisdiction for three reasons: (1) the distance between defendant\'s headquarters in Japan and the Superior Court of California and the unique burdens of submitting a dispute between two foreign nationals in a foreign legal system; (2) California\'s and the foreign plaintiff\'s slight interest in having the case heard in California; (3) the affect on the procedural and substantive interests of other nations by California\'s assertion of jurisdiction over a foreign nationals.

4. Cyber Jurisdiction In Information Technology Act, 2000

However, the law has gone much further. It shall also apply to any violation or contravention of the provisions of this Act done by any person anywhere in the world. By means of this provision, the law is assuming jurisdiction over violators of The Information Technology Act, 2000 outside the territorial boundaries of India. This provision is explained perhaps by

\textsuperscript{46} Asahi Metal Industry Company v. Superior Court, 480 U.S. 102 (1987)
\textsuperscript{47} 480 U.S. 102 (1987).
the unique nature of cyberspace, which knows no
boundaries.

The Information Technology Act, 2000 specifically provides
that unless otherwise provided in the Act, the Act also
applies to any offence or contravention there under
committed outside India by any person irrespective of his
nationality. It is however clarified that the Act shall apply
to an offence or contravention committed outside India by
any person if the act or conduct constituting the offence or
contravention, involves a computer, computer system or
computer network, located in India.

The words ‘act’ or ‘conduct’ constituting the offence or
contravention involves a computer, computer system or
computer network located in India are very significant to
determine jurisdiction of the IT Act over acts committed
outside India. For assuming jurisdiction over an act
constituting an offence or contravention under the IT Act,
which is committed outside India, it has to be proved that the
said act involves a computer, computer system or computer
network located in India.

For instance, where a website is created in the US which
contains pornographic material, it shall not give the IT Act
jurisdiction to question the site unless the creation or
maintenance or running of the site involves a computer,
computer system or computer network located in India. But
where the said website uses a server or any other computer
network located in India, the IT Act would assume
jurisdiction to question the website under section 67 of the
IT Act.

---

48 Sec. 1(2) of IT Act, 2000
49 Sec. 75 of IT Act, 2000
Another instance to explain the jurisdiction of the IT Act is where a person from the US hacks a computer system or network in India, section 66 of the IT Act would come into play to punish the accused for hacking because his act involves a computer in India. Similarly, where a person anywhere in the world plants a virus into a computer system located in India, he would be liable under Section 43(c) of the IT Act to pay damages by way of compensation net exceeding Rs. 1 crore to the victim.

Section 75 of the IT Act is restricted only to those offences or contraventions provided therein and not to other offences under other laws such as the Indian Penal Code, 1860. Jurisdiction over other cyber crimes, for instance under the Indian Penal Code, 1860, has to be determined by the provisions of the Criminal Procedure Code, 1973. The fundamental principle on jurisdiction is the same under the IT Act and the Criminal Procedure Code, 1973, though stated differently. The basic legal principle of jurisdiction under the Code of Criminal Procedure, 1973 is that every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.

In a case where an act is an offence by reason of anything, which has been done and of a consequence, which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such act has been done or such consequence has ensued. For instance, in a case of defamation, either of the courts, i.e. of the place from where the defamatory letter was e-mailed and the place at which it

---

50 Sec. 1(2) r/w Sec. 75 of IT Act, 2000
51 Sec. 177 of Cr. P.C., 1973
52 Sec. 179 of Cr. P.C., 1973
was published or received, if different, shall have jurisdiction to inquire and try the same.

To cite another instance; where in pursuance of misrepresentation by A through e-mail from place X, property was delivered at place Y, A can be tried for the offence of cheating either at place X or Y. In a case where a person in Bombay does an act of hacking of a computer system located in Delhi, he may be tried either in Bombay or Delhi.

In a case where an act is an offence by reason of its relation to any other act which is also an offence or which would be an offence if the doer was capable of committing an offence, the first mentioned offence may be inquired into or tried by a court within whose local jurisdiction either of the acts was done. For instance, in a case of manufacture of substandard fertilizer in place X, which is marketed through e-commerce at place Y, prosecution can be launched at either of the said places because the marketing of the sub-standard fertilizers is an offence by reason of sub-standard manufacture.

The law of jurisdiction stated in the Criminal Procedure Code, 1973 and Section 75 of the IT Act, 2000, as discussed herein, is clear, specific and covers different situations which are likely to generally arise in cyber crime cases. The internet by its nature and purpose operates when the parties interacting or transacting are not physically face to face with one another.

Due to the global access of the internet, cyber crimes generally tend to transcend or disregard geographical boundaries. These factors imply that in most cases of cyber crime, except where insiders are involved, there would be two or more places, one from where the cyber criminal
inflicts the injury—for instance hacks, and the place where the injury is inflicted—for instance at the location of the victim computer, which is hacked. This is in contrast to traditional crimes of rape, murder and kidnapping where the criminal and the victim are at the same place. Moreover, every criminal makes all possible attempts to conceal his identity and place of operation. Alibi is a common defense in criminal matters.

This basic tendency of a criminal coupled with the permissible anonymity provided by the internet makes the cyber criminal almost invisible. Thus, in terms of practical application of the law of jurisdiction over cyber crimes, in most cases, the place of jurisdiction shall be where the victim is inflicted with the injury, whether personally, for instance by fraud, or on his computer, computer system or computer network.

5.7. Judicial Trends in India

It must be stated that Indian case law on cyber jurisdiction of the courts was almost non-existent until the Information Technology Act, 2000 was enacted and enforced on October 17, 2000. The development of information technology as a faster and quicker means of communication in the new millennium has led to certain unforeseen consequences resulting in cybercrimes coming before the Courts for adjudication.

- **Judicial Response on Online Fraud**

The term ‘Internet Fraud’ is very comprehensive but has not been specifically defined under the IT Act. This term will possibly include other crimes also which have been expressly defined in the IT Act. The frauds through Internet
Frauds will take a variety of forms and their classification cannot be easily maintained. The courts in America are busy to resolve Internet frauds.

- **Judicial Response on Credit Card Fraud**

Credit card fraud is a wide ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorised funds from an account.

The credit card frauds have assumed dangerous proportion throughout the globe. In USA, the ten most frequent fraud reports involve undelivered services, damaged, defective, misrepresented or undelivered merchandise, auction sales, pyramid schemes and bogus marketing of goods and of the most predominant among them is credit card fraud. It is estimated that half of a billion dollars are lost by the consumers through credit card frauds.

- **Judicial Response on Defamation**

Every person has a right to have his reputation preserved inviolate. This right of reputation is acknowledged as an inherent personal right or every person. It is a jus in rem, a right good against the entire world. A man’s reputation is his property, more valuable than other property.\(^{53}\)

According to Wikipedia, Cyber Defamation is a crime conducted in cyberspace, usually through the Internet, with the intention of defaming others. Sending defamatory email, writing derogatory comments on facebook, orkut or other social networking sites also constitutes cyber defamation.

---

\(^{53}\) Dixon v. Holden, (1869) LR 7 Eq 488
The Internet can be used to spread misinformation, just as easily as information. Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators. Minors are increasingly using web forums and social networking sites where such information can be posted as well. Criminal behavior can include the publication of intimate photographs or false information about sexual behaviour.

- **Judicial Response in Protection of Intellectual Property Rights**

The judiciary has always responded to the need of the changing scenario in regard to development of technologies. It has used its own interpretative principles to strike a balance between the age-old rigid laws and the advanced technological knowledge. Internet and other information technologies have brought with them certain issues which were not foreseen by the legal regime earlier. Various new developments leading to different kinds of cybercrime unforeseen by the Parliament have come to fore in the new millennium. As regards the internet related IPR disputes arising as a result of development of computer science, the courts have played a role of an umpire between the contesting litigants so as to ensure that no injustice is caused to anyone.

The concept of intellectual property comprises a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights, is an offence punishable under Section 43 of the Information Technology Act, 2000. Software piracy is a common form of IPR violation. Some other IPR violations include copyright infringement,
trademark and service mark violation, theft of computer source code etc. The relevant case law indicating judicial trend in regard to online IPR violations and offences are briefly discussed in the succeeding paragraphs.

- **Judicial Response on Copyright Violation**

Copyright infringement (or copyright violation) is the unauthorised or prohibited use of works covered by copyright law, in a way that violates one of the copyright owner’s exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works.

In *Lotus Development Corporation v. Pareerback Software International*\(^{54}\) it was held that commuter programs like any other works are copyrightable.

- **Judicial Response on Cyber Squatting**

USA has passed an Act known as Anti-Cyber Squatting Consumer Protection Act 1999 to deal with this problem. Cyber squatting according to the United States federal law known as the Anti-cyber squatting protection act, is registering, trafficking in, or using a domain name with bad faith internet to profit from the goodwill of a trademark belonging to someone else. The cyber squatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price\(^{55}\)

- **Judicial Response on Phishing:**

According to Wikipedia phishing means, in the field of computer security, phishing is the criminally fraudulent

\(^{54}\) (1990) 240 F. Supp. 37 (US)
\(^{55}\) Karnika Seth: Cyber Laws in the Information Technology Age, Edn. Ist 2009, Lexis Nexis Butterworths Wadhwa Nagpur, p- 452
process of attempting to acquire sensitive information such as username, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit cards details, by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering.

Under the IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008 Section 66-D is applicable and Section 379 & 420 of Indian Penal Code, 1860 are also applicable.

- **Judicial Response on Online Gambling**

Gambling in India is prohibited under the Public Gambling Act 1867. However the word ‘gambling’ is not defined in the Public Gambling Act 1867. According to the Supreme Court of India, —Gaming is the act or practice of gambling on a game of chance. It is staking on chance where chance is the controlling factor. Internet gambling is traditional crime of gambling where computer is used as tool provided it is otherwise is an offence in a particular jurisdiction.56

There are thousands of Websites that offer online Gambling. The special issue with online gambling is that it is legalised in several countries. So legally the owners of these websites are safe in their home countries. Virtual casinos, Cases of money laundering etc are online cases.57

---

56 Balwinder Kaur: Internet Gambling, Criminal law Journal, October 2008- Journal Section
The law related to gambling is also applicable to online gambling. All gambling contracts are considered to the wagering contracts and it is not possible to enforce such contract under the ICA, detailed above.

- **Judicial Response on Cyber stalking**

Stalking in common parlance means a harassing or threatening behavior which an individual exhibits towards the other. If an individual uses cyberspace for stalking then it is called cyber stalking. Thus, cyber stalking is an online course of conduct of a person by which the targeted person is terrorized, embarrassed, ashamed, molested, outraged, or frightened.

Stalking is not a new phenomena. This offence was being perpetrated in real space also. The stalking by former friends or employees or by a man to women has been in practice with a desire to force the targeted party to come to the terms of stalker. The use of cyberspace for stalking has not only widened the reach of the stalker, as he can now reach to any part of the globe, but he can now impersonate the victim to harass or humiliate him. It is now not necessary for stalker to disclose his identity.

- **Judicial Recognition to Electronic Documents**

Consequent to passing of the Information Technology Act, 2000, electronic documents have come to be recognized at par with the written documents for the purpose of evidence in law. Similarly, the digital signatures\(^\text{58}\) affixed in accordance with the provision of Section 5 of the IT Act, 2000, will be considered equivalent to written signatures. All

\(^{58}\) The expression _Digital Signature_ has been replaced by the term _Electronic Signature_ by the I.T. (Amendment) Act, 2008.
electronic documents either in the electronic form itself or as certified print-out thereof shall be admissible under the Indian Evidence Act 1872. The recognition of electronic document as a valid evidence admissible under the law of evidence has been facilitated the prosecution of cyber criminals and establishing their guilt on the basis of such evidence.

Having referred to the legal provisions relating to the judicial recognition of the electronic record/document as a valid piece of evidence, it would be pertinent to refer to some of the judicial decisions where evidence was produced before the court in one or the other electronic form.

- **Judicial Response on Hacking (Unauthorised Access)**

  Hacking means unauthorised access to computers. When a 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 with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, he is said to have committed an offence of hacking. The person who commits an offence of hacking is called hacker. Webster’s Dictionary defines the term ‘hacker’ as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance

---

59 Section 66 of the IT Act, 2000
Judicial Response on E-Mail Misuse

Electronic mail properly called as e-mail has become most popular and convenient mode of communication. It has, however, serious limitations. It can be intercepted and modified, changed or altogether altered by the interloper. The changes thus made cannot be detected. The sender of the mail can hide his identity. Technologically it is possible to make an e-mail appear to have come from third person. This flexibility in communication has paved the way for e-mail misuse. Nowadays, emails are being used to perpetrate frauds, scams, terrorist activities and other heinous crimes. A good number of cases have been decided in America pertaining to e-mail abuse.

Judicial Response on Illegal Online Selling

It is becoming increasingly common to find cases where sale of illegal articles such as counterfeit currency, counterfeit branded products, narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc. It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button. The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

5.8. Conclusion

A critical evaluation of the case-law referred to above, makes it abundantly clear that operation of global networks
and the concept of quasi-physical territory associated with cyberspace, call upon the need for a new legal perspective and pragmatic approach in handling cyber related crimes by the judiciary. With the tremendous growth of ecommerce, e-banking and e-service regime, the law applicable and administered to cyberspace crimes should be in tune with legal requirements for avoiding the vagaries and discrepancies of national administration of justice system, be it criminal or civil.

There has been significant change in the judicial trend with regard to adjudication of cybercrime during the past two decades. Realising the fact that data stored, processed and transmitted in the electronic form is not directly tangible; the courts while adjudicating on cyber cases no longer adhere to strictly rigid and literal interpretation of law but adopt a more pragmatic and practical approach to the problems involved in the case before them for disposal, without, however, deviating from the basic intent of the legislature in enacting the law applicable to the case. 

In view of the expanding dimensions of cybercrimes in India in recent years, it is not only the police force but also the judicial officers at the lower as well as higher level, who need to be properly educated and trained in various technological aspects of cybercrimes. In the present scenario, the perpetrators of these crimes are moving much faster than the law enforcement agencies in exercising effective control over them. The need of the time therefore, is that the judiciary should move faster than the law enforcement agencies in excersing effective control over them. The need of the time therefore, is that the judiciary should move faster than the cyber criminals by expediting disposal of cyber cases within a time-frame and make sure
that the guilty do not escape punishment due to vagaries of law and evidence. As it has been rightly said, the threat at present is not from the intelligence of the cyber criminals but it is from the ignorance and lack of will to fight against cyber criminality. It may be reiterated that computer is a tool as well as a target for the preparation of cybercrime. The Information technology Act, 2000 specifies the illegal acts which have been made punishable as offences under the Act. The amendments made in the Indian Penal Code, law of Evidence and Criminal Procedure, Banker’s Book Act and the Negotiable Instruments Act also enable the law enforcement agencies and the judiciary to nab cyber criminals promptly and punish them.

The statistical data of cybercrime in India indicates that the incidents of these crime is constantly on an increase as compared to the rate of conviction which is significantly low the reason being that there is general lack of awareness about the computer crimes among the people who at times even do not know that they have fallen a victim to the illegal activities of perpetrators of cybercrime. In result, most of the crime remain unreported, and a few which are reported, result in acquittal due to ignorance of the police and investigating officials about the technicalities of these crimes and lack of sufficient evidence against the accused.

Realising the problem to and handicaps of the police, law enforcement agencies and prosecutors in handling cybercrime investigation due to inadequate knowledge and skill in this hi-tech field, Justice Yad Ram Meena, the Chief Justice of Gujarat High Court suggested that a forensic science University be set up in the State which will help the investigating officials and the judges to unravel vital clues in solving cybercrimes, economic offences and crimes
committed by using sophisticated technology. It would also help in speeding up judicial proceedings. The conduct of judicial trial by video-conferencing has already commenced in major cities in India, which will gradually pick up momentum with the necessary infrastructure and equipment facilities being made available in court-rooms, police stations, prisons and lawyer’s chambers. Recourse to video-conferencing and similar new technologies will develop the law enforcement’s capability to stay abreast new cybercrimes such as encryption etc. and it will go a long way in improving the quality of justice particularly, in reducing costs and delays in disposal of cases specially, the computer related offences.

One of the cyber law experts and Supreme Court lawyer Mr. Pavan Duggal has suggested that there is urgent need for special tribunals being set up headed by well equipped and properly trained Judges to deal solely with cybercrime cases. Another cyber law specialist Shri Prathmesh Popat practicing in Mumbai has underlined the need for computer friendly lawyers and Judges who are well versed with the functioning of the computer system and its operational pitfalls to handle cybercrime cases.

*****
VI

INVESTIGATION ON CYBER CRIMES

With the advancement of technology, every individual person has accessed to internet. The internet thus has become the largest and richest source of information there ever was, with even more systematic and highly refined search engines being developed, getting information (even though it may be restricted) has become easier than it ever was. This increase in the availability of the internet and has also seen a proportional rise in the amount as well as the magnitude of internet related crimes. Therefore, this bring us to the topic Cyber Crime Investigation.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cyber Crimes in India has been evolving rapidly in the 21st century. Technical support scams, along with impersonation of the IRS, are among the most common forms of confidence tricks used in order to receive money from unsuspecting victims.

Unfortunately, with technology on the rise, there’s more room for cyber crime in 2019. According to the Cyber Security Breaches Survey 2018, 43% of businesses were a victim of a cyber security breach in the last 12 months. In the 2017 Official
Annual Cybercrime Report, it’s estimated that Cyber Crime will cost $6 trillion (42,46,86,00,00,00,00,000.06 Indian Rupee) annually by 2021. In 2015, that figure was $3 trillion (21,23,25,00,00,00,000.03 Indian Rupee).

It usually transgress geographical boundaries. With the increase in the domain of the internet, it is possible for a person sitting in Colombia hack into someone’s account in Afghanistan. Therefore, to combat Cyber Crimes, the CBI has created a specialized structure. This includes:

- Cyber Crimes Research and Development Unit (CCRDU)
- Cyber Crimes Investigation Cell (CCIC)
- Cyber Forensics Laboratory
- Network Monitoring Center

6.1. Cyber Crimes Research and Development

The cyber crimes research and development unit has given the responsibility of keeping track of the deployments and changes that take places in this ever-changing area. This involves-

- Ensuring cooperation and ties-ups with the State Police Forces.
- Collection of information about cases of Cyber Crimes reported to the police investigation.
- It ties up with Software Experts to locate and identify areas where the attention of state police is required.
- It entails the collection of information relating to cases that happened in other countries and preparation of a monthly Cyber Crimes Digest.
6.2. Cyber Crime Investigation Cell

The CCIC was established in the month of September 1999. However, it came into action only from March 2000. It acts as a part of the economic offences division and has an all India jurisdiction.

Thus, it can investigate Cyber Crimes under the Investigation Technology Act 2000. It is also a round-the-clock nodal point of contract for Interpol to report cyber crimes in India and is also a member of “Cyber Crime Technology Information Network System” Japan.

6.3. Cyber Forensics Laboratory

The CBL was established in the month of November 2003 and it takes care of the following functions:

- Providing media analysis in support of the criminal investigations by CBI and other Law Enforcement Agencies.
- Providing on-site assistance for computer search and seizure upon request.
- Providing experts testimony.
- Providing adequate Research and Development In Cyber Forensics.

The information so collected is to be used as evidence in court.

The purpose of CBL is to police the internet to ensure that certain Cyber Crimes can be stopped before their commission. For this Network Monitoring Center has been provided with a Network Monitoring Tool, developed by I.L.T. Kanpur. It is also used to allow similar tools to achieve such a purpose.
Today with the growing arms of cyber space the territory boundaries seem to disappear and the concept of territorial jurisdiction as envisaged under Section 16 of Criminal Procedure Code (Courts of Metropolitan Magistrate) and Section 2 of the Indian Penal Code (Punishments of Offences Committed Within India) will have to give way to alternative method to dispute resolution.

Karnataka was the first to establish a dedicated police station to handle digital crime 15 years ago. Other states including Uttar Pradesh and Maharashtra, have stepped up police training, including seeking out experts from industry.

Recently, on October 2, 2018, the SBM had issued a statement confirming that its India operations had been hit by a cyber fraud with a potential loss of around $14 million (99,09,76,000.00 Indian Rupee). It had said that some unknown persons hacked into the bank's servers to illegally access various accounts and managed to transfer the monies to multiple accounts outside the country. It was the second major cyberattack on a bank in Maharashtra in the past couple of months.

In two cyberattacks on August 9 and 11, 2018, the Cosmos Bank Pvt Ltd, Pune, lost a total of Rs 94.24 crore to an international group of operatives working in tandem in several countries.

The Ministry of Electronics And Information Technology (MEITY) has collaborated with The Data Security Council Of India (DSCI) to set up cyber forensic labs in all metro cities for training and building awareness of cybercrime investigation. Kunal Kumar, chief technology officer at Digital Task Force, a cyber-security company, said, “Policemen are regularly upskilled and updated about
emerging technologies. States such as Maharashtra and Delhi have good infrastructure, but it still falls short when compared to the technology industry.”

The following measures are being taken by the government to tackle Cyber Crimes:

- The Ministry of Home Affairs has issued an advisory to the State Governments and Union Territory Administrations on Cyber Crime, to build adequate technical capacity in handling Cyber Crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of Cyber Crimes.
- A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Courts.
- Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
- Cyber Forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.
In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber Crimes for judicial officers.

Government has decided to provide a centralized citizen portal through Crime and Criminal Tracking Network and Systems (CCTNS) for registering online Cyber Crime complaints.

The Ministry of Home Affairs has also in-principle approved to set up an Indian Cyber Crime Coordination Centre (I4C) to fight against Cyber Crime in the country and establish an open platform for victims to raise cybercrime complaints with the protocol for resolution such as online crime reporting, to support and coordinate electronic investigations of cybercrime, assist the law enforcement agencies in criminal investigation etc.

The cyber space is being closely monitored by the Government in respect of the situation of radicalization attempts. The Government has also directed the intelligence agencies to identify potential recruits and keep them under surveillance.

Though not all people are victims to Cybercrimes, they are still at risk. Crimes by computer vary, and they don’t always occur behind the computer, but they executed by computer. The hacker’s identity is ranged between 12 years young to 67 years old. The hacker could live three continents away from its victim, and they wouldn’t even know they were being hacked. Crimes done behind the computer are the 21st century’s problem.
With the technology increasing, criminals don’t have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren’t guns anymore; they attack with mouse cursors and passwords.

*****
"Today, we face another major potential attack on our country. This attack is not a hijacked plane or bomb, although that remains a threat, rather, it is a cyber attack."

`Akash Kamal Mishra`