CYBER LAW & ETHICS

BCSF188OEF

STUDY MATERIAL

BE – IV Year (VIII Semester)

(2021-2022)

DEPARTMENT OF CSE

SRI CHANDRASEKHARENDRA SARASWATHI VISWA MAHAVIDYALAYA

(Deemed to be University established under section 3 of UGC act 1956)

ENATHUR, KANCHIPURAM - 631 561

Course Code:	CYBER LAW AND ETHICS	L	T	P	C
BCSF188OEF		3	0	0	3

PRE-REQUISITE

1. Cryptography and Network Security.
2. Ethical Hacking

OBJECTIVES

1. To understand the basics of cyber threats & security.
2. To learn various fundamentals of law & act
3. To study about cyber & security policies.
4. To understand the nature and applications of cyber law in real life
5. To understand various security issues in cyber.

COURSE OUTCOMES

1. Basic information on cybercrime.
2. Cyber laws for various crime activities.
3. Identify the security policies for cyber issues.
4. Analyze the role of organization for securing cyberspace.
5. Need for security in organizations.

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M									
CO2		M								
CO3			L							
CO4				S						
CO5					M					

S- STRONG, M -MEDIUM, L- LOW

UNIT – I INTRODUCTION

Introduction, Forgery, Hacking, Software Piracy, Computer Network intrusion - Category of Cybercrime - Cybercrime Mobile & Wireless devices - Tools and Methods used in Cybercrime - Phishing & Identity Theft.

UNIT – II CYBER CRIME

Constitutional & Human Rights issues in cyberspace freedom of speech and Expression in cyber space, right to access in cyber space-access to internet, right to privacy, right to data protection cybercrimes and legal framework, cybercrime against individual, institution and state, Hacking Digital Forgery cyber stalking/Harassment, Cyber Pornography, identity theft & fraud, cyber terrorism, cyber defamation.

UNIT - III CYBER LAW

Cyber torts cyber defamation, different types of civil wrongs under IT Act 2000, Intellectual property issues in cyber space, interface with copyright law, interface with patent law, trademark & domain names related issues.

UNIT - IV E-COMMERCE

E-commerce concept-commerce-salient features online approaches like B2B, B2C & C2Conline contracts, click wrap contracts, applicability of Indian contract act 1872.

UNIT – V JURISDICTION

Dispute Resolution in cyberspace, concepts of Jurisdiction, Indian context of Jurisdiction and IT Act 2000.Interantional Law and Jurisdictional issues in cyberspace.

TEXT BOOKS

Chris Reed & John Angel, Computer Law, OUP, New York.

Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co, New Delhi.

Verma S, K, Mittal Raman, Legal Dimensions of Cyber Space, Indian Law Institute.

Jonthan Rosenoer, Cyber Law, Springer, New York.

Sudhir Naib, The Information Technology Act, 2005: A Handbook, OUP, New York.

S. R. Bhansali, Information Technology Act, 2000, University Book House Pvt. Ltd.

REFERENCES

Reich, Pauline C, "Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization", IGI Global, 2012.

Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, "Cyber Security Policy Guidebook", John Wiley & Sons, 2012.

VivekSood, "Cyber Law Simplified", Tata Mcgraw Hill, 2001.

Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global, 2009.

Jonathan Rosenoer, “Cyber law: the Law of the Internet”, Springer - verlag, 1997.

UNIT I

Introduction to Cyber Law

What is Cyber Law?

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

Need for Cyber Law:

TACKLING CYBER CRIMES

INTELLECTUAL PROPERTY RIGHTS AND COPYRIGHTS PROTECTION ACT

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.
3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
4. Cyberspace is absolutely open to participation by all. A ten-year-old in Bhutan can have a live chat session with an eight-year-old in Bali without any regard for the distance or the anonymity between them

Hacking:

- role of an ethical hacker
- legally as an ethical hacker

Ethical hackers

- Employed by companies to perform penetration tests

Penetration test

- Legal attempt to break into a company's network to find its weakest link
- Tester only reports findings, does not solve problems

Security test

- More than an attempt to break in; also includes analyzing company's security policy and procedures
- Tester offers solutions to secure or protect the network

Role of Security & Penetration Testers:

- Hackers
  - Access computer system or network without authorization
  - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
  - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities but with owner's permission

Tiger box

Collection of OSs and hacking tools

Usually on a laptop

Helps penetration testers and security testers conduct vulnerabilities assessments and attacks

Penetration Testing Methodologies:

White box model

Tester is told everything about the network topology and technology

- Network diagram

Tester is authorized to interview IT personnel and company employees

Makes tester's job a little easier

- Black box model
  - Company staff does not know about the test
  - Tester is not given details about the network
    - Burden is on the tester to find these details
  - Tests if security personnel are able to detect an attack

Gray box model

Hybrid of the white and black box models

Company gives tester partial information

Overview – Software Piracy

- Software piracy is illegal copying of computer software, and it is a prevalent and serious problem or sale of saleable software without a license.
- Major software companies are losing 35-40% of their potential retail revenue to software pirates around the world

The Concept of privacy

- Unreasonable intrusion upon a person's seclusion
- Public disclosure of private facts
- Publicity that places a person in false light
- Appropriation of a person's name or likeness invoked

Right to privacy in India

- Article 21 of the Constitution of India-Right to life and personal liberty by necessary implication confers right to privacy –
- Kharak singh v State of U.P AIR 1963 SC 1295
- Gobind v State of M.P 1975 SCC 468
- PUCL v UOI (1997) 1 SCC 318
- R.Rajagopal v State of Tamil Nadu (1994)6 SC 632-autoshanker case
- Article 19-freedom of speech and expression
- Article 19(2) –Reasonable restrictions
- One of the restrictions/conditions is National Security

- Privacy vs national security balancing competing interests

Threats to privacy

- Hacking
- Cookies
- HTTP
- Information provided voluntarily
- Browsers
- E-mail
- Websites
- Spam
- Software's to check employee behavior
- Satellite vigilance

Protecting privacy

- Encryption
- Trust mark-webtrust, truste,etc
- Anonymity
- Cookie guards-cookie cop, siemen's webwasher, cookie crush,etc
- Privacy policy of website-p3p-platform for privacy preference
- Secure system for electronic money transfer- e.g SSL
- Need for legislation and enforcement
- Establish effective dispute resolution

What is a Mobile Device/Wireless?

- Mobile Device: a device that is easy to use, enables remote access to business networks and the internet, and enables quick transfer of data.
- Wireless Communication: the transfer of *information* over a distance without the use of electrical conductors or wires

Examples of Mobile Devices

- Laptops

- Cell Phones
- PDAs
- Flash Drives
- Bluetooth
- Mouse/Keyboard
- Mp3 Players

How does Wireless Work?

- Wireless networks use electromagnetic radiation as their means of transmitting data through space.
- An access point (AP) device is physically connected to the LAN (typically a router)
- The AP has an antenna and sends and receives data packets through space
- A wireless device then connects to the WLAN using its transmitter to connect to the AP, and then to the LAN.

What are the Advantages?

- Enhanced productivity
- Portability: Stay connected even away from home or office, resulting in a more flexible work life

Risk: Physical theft/loss of device

- Laptop theft accounted for 50% of reported security attacks.
  CSI, The 12th Annual Computer Crime and Security Survey, 2007
- Lost or stolen laptops and mobile devices are the most frequent cause of a data breach, accounting for 49% of data breaches in 2007.
  Ponemon Institute, U.S. Costs of a Data Breach, November 2007

Mitigation

- Cable Locks
- Never leave hardware unattended
- Make hardware as inconspicuous as possible
- Invest in tracking/recovery software
- Encryption
- Authentication

Risk: Data loss/leakage

- 7 out of 10 government mobile devices are unencrypted.
  Government Accountability Office (GAO), IT Security: Federal Agency efforts to encrypt sensitive information are under way, but work remains, June 2008
- The cost of recovering from a single data breach now averages $6.3M - that's up 31 percent since 2006 and nearly 90 percent since 2005.
  Ponemon Institute, U.S. Costs of a Data Breach, November 2007

Wireless networks

- Infrastructure Mode
- Ad-hoc mode

Specific Threats to Wireless Networks

- Unauthorized use of service
- Jamming
  - Constant Jamming
  - Deceptive Jamming

Auditing Wireless Networks

- Access control, transmission control, viruses, and monitoring access points are important risks to consider
- Firewall generally secures information but WLAN creates new challenges because it easier to access. Therefore, control is more important.
  - (Ex) If an employee were to bring in an unauthorized router in to work, unauthorized users could potentially access the network from outside the building
- Access Point (AP) – security of APs is crucial for wireless network auditing, consider unauthorized access, unauthorized APs, improperly configured APs, and Ad Hoc networks
- An Auditor might walk around the building looking for markings left on the ground by hackers indicating a spot in range of a wireless network
- Wireless auditor – an automated system that detects anomalies

Tools and Methods used in Cybercrime

Various types of Cybercrime attack modes are

1) Hacking

2) Denial Of Service Attack

3) Software Piracy

4) Phishing

5) Spoofing.

Some important tool use for preventing cyber-attack is

1)Kali Linux

2) Ophcrack

3) EnCase

4) SafeBack

5) Data Dumber

Purpose of Proxy Server

- Improve Performance
- Filter Requests
- Keep system behind the curtain
- Used as IP address multiplexer
- Its Cache memory can serve all users
- The attacker first connects to a proxy server – establishes connection with the target through existing connection with the proxy.

An Anonymizer

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.

It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.

It accesses the Internet on the user's behalf protecting personal information by hiding the client computer's identifying information.

Phishing and Identify theft:

Stealing personal and financial data with virus infected system as a method of online ID theft

Phishing works with planning, setup, attack and collection of information recorded from the online communication.

UNIT II

Cybercrime – An Introduction

Computer Crime, E-Crime, Hi-Tech Crime or Electronic Crime is where a computer is the target of a crime or is the means adopted to commit a crime.

Most of these crimes are not new. Criminals simply devise different ways to undertake standard criminal activities such as fraud, theft, blackmail, forgery, and embezzlement using the new medium, often involving the Internet

Computer vulnerability

- Computers store huge amounts of data in small spaces
- Ease of access
- Complexity of technology
- Human error
- One of the key elements that keeps most members of any society honest is fear of being caught — the deterrence factor. Cyberspace changes two of those rules. First, it offers the criminal an opportunity of attacking his victims from the remoteness of a different continent and secondly, the results of the crime are not immediately apparent.
- Need new laws and upgraded technology to combat cyber crimes

Types of Cyber crimes

- Credit card frauds
- Cyber pornography
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Defamation
- Cyber stalking (section 509 IPC)
- Phishing

- Cyber terrorism

TYPES OF CYBER CRIMES

E-Mail bombing: Email bombing refers to sending a large number of e-mails to the victim resulting in interruption in the victims' e-mail account or mail servers.

Data diddling: This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

Salami attacks: These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer

Denial of Service: This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

Cyber Crime Data in Regional Context

Carding:

Carding is a serious threat to India, as it does not require a high degree of sophistication and is considered particularly pernicious by international financial institutions and e-commerce providers.

Bots:

Bots, compromised servers that may be launching cyber-attacks or sending Spam, were detected in the India IP space, including servers with the domain name.

Phishing:

ISPs were able to point to a few examples of phishing capture sites being located on their servers, one targeting eBay (a frequent attack point for phishers).

Constitutional & Human Rights issues in Cyberspace

The right includes freedom to receive and impart information and ideas and to hold opinions without any state interference. It also includes the right to express oneself in any medium including exchanging ideas and thoughts through Internet platforms or social networks.

Issues in Cyberspace

Cyberspace has been faced many security challenges like identity tracing, identity theft, cyberspace terrorism and cyberspace warfare. In this paper, we focus on analysis these security challenges, and give some possible solutions offered by law and technology.

Right to use Cyberspace

Accordingly, the Internet has become a major vehicle for the exercise of the right to freedom of expression and information. The International Covenant on Civil and Political Rights (ICCPR)3 states (in article 19(2))

Freedom of expression in Cyberspace

Freedom of speech and expression is broadly understood as the notion that every person has the natural right to freely express themselves through any media and frontier without outside interference, such as censorship, and without fear of reprisal, such as threats and persecutions.

Freedom Of Speech in Cyberspace

Freedom of speech is one of the human rights inherit by human in the world as stated in Article 19 of the UDHR (Universal Declaration of Human Rights), the article states that everyone has the right to freedom of opinion and speech, including the right to hold opinions without interference and to seek, receive and convey information and ideas through any media regardless of boundaries (region).

The freedom of speech rights in regard of speaking and giving opinion which associated with IT is often leads to victim suspected of breaking these limits. Actually, the freedom of speech rights itself is regulated in the article 28 of the 1945

Right to access in Cyberspace – an Internet

Right to internet under **Article 21**

The court took the view that the right to be able to access the internet has been read into the fundamental right to life and liberty, as well as privacy under Article 21. The court added that it constitutes an essential part of the infrastructure of freedom of speech and expression.

Internet plays a significant role with the escalation of technology, so a primitive question arises that:

Whether or not Internet access should be considered a civil right?

In 2016, the UNHRC General Assembly expressed an important human right to Internet access.

The Internet is the undiscovered ocean of information, and the biggest supplier in the world.

Technology is, in his opinion, an enabling agent of rights and not a privilege of its own. India has legislation which deals with cyberspace crimes.

Right to privacy

What is privacy?

Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.

Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps to establish boundaries to limit with the access for information sharing and communication.

Privacy is an essential way to protect against society with arbitrary and unjustified usage of power. Privacy International envisions, protects the right to access the information. Individual can participate in the modern development of technologies with ability to freely enjoy the rights. Privacy is a qualifies, fundamental human right with articulated management instruments.

Right to data protection

Personal data is any information related to privacy, professional or public. In the recent environment, vast amount of personal data are shared and transferred around the globe instantaneously. Data protection refers to the practices, safeguards and binding rules with protection of personal information.

Data Protection Laws:

- Laws need to be updated to address today's reality

- Corporate co- and self-regulation is not working to protect the data

Cybercrime and Legal frameworks

Cybercrime is defined as a crime in which a computer can commit with hacking, phishing and spamming as a tool to work as offense. Cybercriminals use computer technology to access personal information, business trade for exploitative purposes. Criminals can perform illegal activities referred as hackers.

Cybercrime include online bank information theft, identity theft, unauthorized computer access.

Types of Cybercrime

- DDoS Attacks
- Botnets
- Identity Theft
- Cyberstalking
- Social Engineering
- PUPs
- Phishing
- Prohibited/Illegal Content

Cybercrimes against Individuals, Institution and State

- Individual
- Property
- Government

Individual: This type of Cybercrime can be in the form of Cyberstalking, distributing pornography, trafficking and "grooming".

Institutions: It includes, financial institutions, banks with highly affected event of cyber-attacks such as data breaches. The institutions have to pay fines and penalties for losing personal identifiable information.

Hacking

It can be worked out with identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Hacking causes computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data.

Digital Forgery

Forgery has been defined as the crime of falsely altering document with intension to mislead others. It includes the production of counterfeited items. Digital Forgery involve electronic forgery and identity theft. The majority of digital forgery occurs because of digitally altering pictures. Digital techniques are notoriously more precise than conventional retouching because any area of the photo can be changed pixel by pixel. The three types of image forgery include image retouching, splicing forgery and copy-move image forgery.

Cyberstalking

- Cyberstalking is a new concept with agreed-upon definition such as
- Stalking is done with the assistance of technology
- It is done to make a person feel afraid, threatened or worried about their safety
- It invades a person's privacy
- The stalker monitors the victim's behaviour, threatens them with unwanted access.

Cyber pornography

It is defined as the act of using cyberspace to create, display, distribute, import or publish pornography. The traditional pornographic content has been largely replaced by online/digital pornographic content.

Cyber Defamation

The term defamation is used to define the injury caused by the reputation of a person. The intention of the person causes defamatory statement which lowers the reputation of the person against whom the statement has been made in the eyes of general public. Defamation is the application to Cyber defamation which involves defamation of a person through a new and a virtual medium. Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.

Medium by which offense of cyber defamation can be caused:

- World Wide Web
- Discussion groups
- Intranets
- Mailing lists and bulletin boards
- E-mail

UNIT III

Cyber torts – An Introduction

Cyber Torts

A tort is a negligent or intentional act is done by someone that injures someone else in some way. Cyber Torts are simply a tort done over cyberspace. Cyber torts are very important because they are on the rise and are still crimes that can have serious effects on society. Everyone should be exposed to the dangers and damages caused by cyber torts because technology is an important aspect in everyone's lives, especially now.

The word "tort" originates from the French language, in English, it is equivalent to term "wrong" and it is derived from the Latin word "tortum" which means "wrong or injury" and the word tortum is developed from the word "torquere" which means "to twist". It is simply a breach of duty which amounts to a civil wrong.

A person who commits a tort is called as a tortfeasor and if there are multiple persons involved, then they are called joint tortfeasor as they are jointly liable for the tortious act and they can be sued individually or jointly.

Essential elements of a tort

- A Wrongful act
- A duty imposed by the law
- The act must give rise to legal or actual damage

Various Kinds of cyber torts

Cyber Stalking

Cyberstalking involves following a person's online presence on various social media or other websites, by posting messages which can be threatening also as well as posting on bulletin boards.

Harassment via e-mails

Harassment via emails is a very old concept and has been there since the initial days of electronic mails, it is very much similar to the concept of harassment vialetters in real life.

Cyber Obscenity

Pornography on the internet has various forms. It may also include prohibited material such as child pornography, which is a heinous crime in real life as well.

Cyber Defamation

Defamation is an act of making a statement about an individual which may lower his reputation in the eyes of the right-thinking people. It can be written and oral also. Cyber defamation is very similar to defamation in real life except for the involvement of a virtual machine. Cyber defamation is that kind of defamation which is done through the virtual medium.

Cyber-Vandalism

Conventional vandalism means to deliberately destroy or damage the property ofsomeone. Thus, cyber-vandalism means to deliberately put any kind of physical harm to anybody's computer or virtual machine. These acts may be in the form of theft of a computer or any peripheral of the computer also.

Trafficking

Trafficking is of many kinds, it may be in drug, ammunition, or even human beings, etc. Trafficking is taken a form with the ascension of the internet as cyber trafficking has also developed, where the process of trafficking is done online through the use of a virtual machine.

Fraud and Cheating

Online fraud and cheating have become one of the biggest threats the governmenthas to deal with. These include Credit card crimes, fake job offerings, misappropriation, etc.

Different Types of Civil Wrongs under the IT Act 2000

Civil Cyber Wrongs A civil cyber wrong is one which is committed online and is civil in nature, such as a tort of defamation committed online through a computer (or any device which has access to the internet and is able to modify the information or post anything online, such as a mobile phone, or a tablet) is used as a tool to commit that kind of wrong. Although not defined or addressed as civil cyber wrongs, the essence of civil liability is defined under section 43 of the IT Act, 2000.

Criminal Cyber Wrongs

A criminal cyber wrong is a serious threat and it must be dealt with as soon as possible, a criminal cyber wrong is a criminal wrong committed online through the use of technology, crimes such as Hacking, information theft, denial of service attacks, etc. Although not addressed as criminal cyber wrongs in any acts, but various wrongs of criminal nature are defined under the IT Act, 2000, such as Child pornography defined under **Section 67-A** of the act.

Intellectual property rights are the legal rights that cover the privileges given to individuals who are owners and inventors of a work. The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO)

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms and broadcasts
- Trademarks, service marks, commercial names and designations

Types of Intellectual Property Rights

Intellectual Property Rights can be further classified into the following categories −

- Copyright
- Patent
- Patent
- Trade Secrets, etc.

Intellectual Property in Cyber Space

- Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.
- To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.
- Today it is critical for every business to develop an effective and collaborative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined. Various approaches and legislations have been designed by the law-makers.

Interface with copyright law

Copyright law is a type of intellectual property law that protects creative works,which can include things like plays, movies, manuscripts, paintings, drawings, songs, letters, and many other things. In the United States, the Constitution provides that copyright law protects "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. Most other countries that are members of the World Intellectual Property Organization (WIPO) have similar definitions. Copyright law does not protect ideas, procedures, methods of operations, or mathematical concepts (though other types of IP may protect them under certaincircumstances). In other words, copyright law is about protecting a particular expression of an idea, not functional elements of a given work.

Interface with Patent Law

Patent law is part of intellectual property law and controls what inventions qualify for patents. A patent is a property right that gives an inventor the legal ability to stop others from making, using or selling an invention for a certain amount of time.

Three types of patents are as follows:

Utility patent

Design patent

Plant patent

Trademark and Domain name issues

Domain Name

A domain name is an Internet resource name that is universally understood by web servers and online organizations and provides all pertinent destination information. To access an organization's Web-based services, website usersmust know the precise domain name.

Domain names are used worldwide, particularly in the world of networks and data communication. The following points explain how they work and how theyare used:

- Domain names have two parts that are separated by a dot, such as example.com.
- A domain name can be used to identify a single IP address or group of IP addresses.
- A host or organization may use a domain name as an alternate IP addressbecause domain names are alphanumeric (as opposed to all numbers), making them easier to memorize.
- A domain name is used as part of a URL to identify a website.
- The part that follows the dot is the top-level domain (TLD), or group towhich the domain name belongs. For example, .gov is the TLD for U.S. government domains.

Domain name issues

Stolen Domain Names

From a legal perspective, this is one of the simplest scenarios in domain name law. If a third party has without any right whatsoever managed to transfer a domain name from your account to its own, then it has infringed your domain rights and you should be able to recover it by contacting the ISP and proving your case. In a world menaced by terrorism and global warming, stolen domain names might not sound like a serious issue but the entities behind such foul playare often serious criminals.

Cybersquatting

This is one of the most common scenarios in domain disputes. This can overlap with passing off domain name activity. In that scenario, the domain name is usually diverted to the website of a third – party competitor who seeks to trade off the goodwill of the legitimate brand owner. However, typically cybersquatting and passing off domain name machinations are quite distinct.

Passing Off Domain Name

This is probably the busiest area of activity for the typical domain name lawyer. Domain name disputes often pivot around the issue as to whether a company has overstepped the mark by registering a domain name which reflects the trading name or product name of one of its competitors. Another similar form of dispute may arise where a company uses metatags or pays for sponsored ads which incorporate the competitor's branding. Each case is assessed on its facts but if the bottom line is that a trading entity is taking unfair advantage of a competitor's branding and/or marketing efforts, the courts will usually find in favour of the competitor and award damages or order an account for profits.

Trademark related issues – Here are ten issues keeping trademark attorneys andrights holders alike, on their toes.

Innovative Trademark Trolling

Just like their patent troll counterparts, individuals and agencies are using predatory

registrations to insidious ends. Unscrupulous characters are exploiting the opportunity to demand licensing fees from alleged infringers.

Trademarks as Keywords

Google's AdWords program empowers advertisers by allowing them to assign keywords to their ads that trigger their appearance in particular search queries. In an effort to interject brand awareness, even in the case of specific queries for competitors, businesses have adopted the practice of tapping competitor's keywords in their AdWords approach. The technique obviously obfuscates the search picture, but, at present, the law current allows the practice, provided the keyword doesn't appear in search links sponsored by advertisers.

UNIT IV

E-Commerce – An Introduction

Ecommerce also known as Electronic Commerce, refers to buying and selling of products orservices over the Internet. Normally ecommerce is used to refer to the sale of physical products online, but it can also describe any kind of commercial transaction that is facilitatedthrough the internet.

The first ever online sale was in 1994 when a man sold a CD by the band Sting to his friend through his website NetMarket, an American retail platform. This is the first example of a consumer buying a product from a business through the World Wide Web or e-commerce as we commonly know it today. After that ecommerce has evolved to make products easier to discover and purchase through online retailers and marketplaces. All freelancers as well as small and large businesses have been benefited from e-commerce which enables them to sell their goods and services at a scale that was not possible with traditional offline retail.

Types of Ecommerce model:

There are basically 4 main types of ecommerce models that can describe almost everytransaction that takes place between consumers and businesses.

1. **Business to Consumer (B2C):**
   When a good or service is sold to an individual consumer by a business, e.g., we buy apair of shoes from an online retailer.

2. **Business to Business (B2B):**
   When a good or service is sold by a business to another business, e.g., a software-as-a-service is sold by a business for other businesses to use.

3. **Consumer to Consumer (C2C):**
   When a good or service is sold by a consumer to another consumer, e.g., we sell our oldfurniture on eBay to another consumer.

4. **Consumer to Business (C2B):**

   When a consumer's own products or services is sold to a business or organization, e.g., an authority offers exposure to their online audience in exchange for a fee or a photographer licenses their photo for a business to use.

Seven Unique features of E-commerce

1. Ubiquity- The traditional business market is a physical place, access to treatment by means of document circulation. For example, clothes and shoes are usually directed toencourage customers to go somewhere to buy. E-commerce is ubiquitous meaning that it can be everywhere. E-commerce is the worlds reduce cognitive energy requiredto complete the task.
2. Global Reach- E-commerce allows business transactions on the cross country bound can be more convenient and more effective as compared with the traditional commerce. On the e-commerce businesses potential market scale is roughly equivalent to the network the size of the world's population.
3. Universal Standards- E-commerce technologies is an unusual feature, is the technical standard of the Internet, so to carry out the technical standard of e-commerce is shared by all countries around the world standard. Standard can greatly affect the market entry cost and considering the cost of the goods on the market. The standard can make technology business existing become more easily, which can reduce the cost, technique of indirect costs in addition can set the electronic commerce website 10$ / month.
4. Richness- Advertising and branding are an important part of commerce. E-commerce can deliver video, audio, animation, billboards, signs and etc. However, it's about as rich as television technology.
5. Interactivity- Twentieth Century electronic commerce business technology is called interactive, so they allow for two-way communication between businesses and consumers.
6. Information Density- The density of information the Internet has greatly improved, aslong as the total amount and all markets, consumers and businesses quality information. The electronic commerce technology, reduce the information collection, storage, communication and processing cost. At the

same time, accuracy and timeliness of the information technology increases greatly, information is more useful,more important than ever.

7. Personalization- E-commerce technology allows for personalization. Business can be adjusted for a name, a person's interests and past purchase message objects and marketing message to a specific individual. The technology also allows for custom. Merchants can change the product or service based on user preferences, or previous behavior.

E-Commerce - B2B Model

A website following the B2B business model sells its products to an intermediate buyer who then sellsthe products to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, it sells the end product to the final customer.

B2B identifies both the seller as well as the buyer as business entities. B2B covers a large number of applications, which enables business to form relationships with their distributors, re-sellers, suppliers, etc. Following are the leading items in B2B eCommerce.

Following are the key technologies used in B2B e-commerce −

- **Electronic Data Interchange (EDI)** − EDI is an inter-organizational exchange of businessdocuments in a structured and machine processable format.
- **Internet** − Internet represents the World Wide Web or the network of networks connectingcomputers across the world.
- **Intranet** − Intranet represents a dedicated network of computers within a single organization.
- **Extranet** − Extranet represents a network where the outside business partners, suppliers, or customers can have a limited access to a portion of enterprise intranet/network.
- **Back-End Information System Integration** − Back-end information systems are databasemanagement systems used to manage the business data.

Following are the architectural models in B2B e-commerce −

- **Supplier Oriented marketplace** − In this type of model, a common marketplace provided by supplier is used by both individual customers as well as business users. A supplier offers an e-stores for sales promotion.
- **Buyer Oriented marketplace** − In this type of model, buyer has his/her own market place or e-market. He invites suppliers to bid on product's catalog. A Buyer company opens a biddingsite.
- **Intermediary Oriented marketplace** − In this type of model, an intermediary company runs

  a market place where business buyers and sellers can transact with each other.

E-Commerce - B2C Model

In B2C model, a business website is a place where all the transactions take place directly between abusiness organization and a consumer.

In the B2C model, a consumer goes to the website, selects a catalog, orders the catalog, and an email is sent to the business organization. After receiving the order, goods are dispatched to the customer. Following are the key features of the B2C model −

- Heavy advertising required to attract customers.
- High investments in terms of hardware/software.

Following are the steps used in B2C e-commerce −
A consumer −

- determines the requirement.
- searches available items on the website meeting the requirment.
- compares similar items for price, delivery date or any other terms.

- places the order.
- pays the bill.
- receives the delivered item and review/inspect them.
- consults the vendor to get after service support or returns the product if not satisfied with the delivered product.

Disintermediation and Re-intermediation

In traditional commerce, there are intermediating agents like wholesalers, distributors, and retailers between the manufacturer and the consumer. In B2C websites, a manufacturer can sell its products directly to potential consumers. This process of removal of business layers responsible for intermediary functions is called **disintermediation**.

What is an Online Contract?

With the advance use of internet and electronic commerce, online contracts have assumed importance mainly in terms of reach and multiplicity. Online contract or an electronic contract is an agreement modelled, signed and executed electronically, usually over internet. An Online contract is conceptually very similar and is drafted in the same manner in which a traditional paper-based contract is drafted. In case of an online contract, the seller who intends to sell their products, present their products, prices and terms for buying such products to the prospective buyers. In turn, the buyers who are interested in buying the products either consider or click on the 'I Agree' or 'Click to Agree'

Once the terms are accepted and the payment is made, the transaction can be completed. The communication is basically made between two computers through servers. The online contract is brought to the scenario to help people in the way of formulating and implementing policies of commercial contracts within business directed over internet. Online Contract is modelled for the sale, purchase and supply of products and services

to both consumers and business associates.

Online can be categorized into three types mainly i.e. browse or web wrap contracts, shrink wrap contracts and clickwrap contracts. Other kinds of online contracts include employment contract, contractor agreement, consultant agreement, Sale re-sale and distributor agreements, non-disclosure agreements, software development and licensing agreements, source code escrow agreements. Though these online contracts are witnessed in our everyday life, most of us are not aware of the legal complexities connected to it; the use of online contract faces many technical and legal challenges.

Types of Online Contract

Online contracts can be of three types mainly i.e. shrink-wrap agreements, click or web-wrap agreements and browse-wrap agreements. In our everyday life, we usually witness these types of online contracts. Other types of online contracts include employment contract, contractor agreement, consultant agreement, Sale re-sale and distributor agreements, non-disclosure agreements, software development and licensing agreements, source code escrow agreements.

What Is a Clickwrap Agreement?

Clickwrap is an online agreement between a user and a company that requires the user to click a box or a button before they download content, make a purchase, or use a website. The box or button confirms that the user agrees to an online contract with the company, and substitutes for the user's signature.

In a clickwrap agreement, in order to use a website or download content, the user has to check a box saying they've read and agree to the terms and conditions that apply to the website or software.

Sometimes the agreements are many pages long and difficult to read. They usually contain two things:

- A checkbox or button
- A notice telling you that you agree to the terms if you click the box Clickwrap agreements are also called:

- Clickthrough agreements
- Clickwrap licenses

Types of clickwrap (and browse wrap) include:

- Terms and conditions
- Terms of use
- Privacy policies
- End user license agreements (EULAs)

Buttons that signify clickwrap agreements include:

- I agree
- OK
- I consent
- I accept

Why Is a Clickwrap Agreement Important?

Clickwrap agreements add convenience for companies in lots of ways:

- Speedy and easy customer agreement
- Not just for software programs but for other kinds of agreements, too
- Simple, encrypted digital contract records
- Automatic downloading of any contract revisions
- e-Signature law and court case compliant

Clickwrap web forms embedded directly into websiteswith clickwrap agreements companies can:

- Have lots of customers sign the same contract without discussing contract terms with any one customer
- Save an electronic signature
- Include terms and conditions that aren't covered by the law

Indian Contract Act, 1872

The Act as enacted originally had 266 Sections, it had wide scope and included.

- General Principles of Law of Contract- Sections 01 to 75
- Contract relating to Sale of Goods- Sections 76 to 123
- Special Contracts- Indemnity, Guarantee, Bailment & Pledge and Agency - Sections 124 to 238
- Contracts relating to Partnership- Sections 239 to 266

UNIT V

JURISDICTION

JURISDICTION

Jurisdiction can be defined as the limit of a judicial authority or the extent to which a court of law can exercise its authority over suits, cases, appeals etc. The rationale behind introducing the concept of jurisdiction in law is that a court should be able to try and adjudicate only in those matters with which it has some connection or which fall within the geographical or political or pecuniary limits of its authority. A 1921 Calcutta High Court judgment in the case of *Hriday Nath Roy* v. *Ram Chandra* sought to explain the meaning of the term 'jurisdiction' in a great detail. The bench observed:

'An examination of the cases in the books discloses numerous attempts to define the term 'jurisdiction',which has been stated to be 'the power to hear and determine issues of law and fact;' 'the authority by which three judicial officers take cognizance of and decide cause;' 'the authority to hear and decide a legal controversy;' 'the power to hear and determine the subject-matter in controversy between parties to a suit and to adjudicate or exercise any judicial power over them;''the power to hear, determine and pronounce judgment on the issues before the Court;''the power or authority which is conferred upon a Court by the Legislature to hear and determine causes between parties and to carry the judgments into effect;' 'the power to enquire into the facts, to apply the law, to pronounce the judgment and to carry it into execution.'

Types of Jurisdictions:

In India, there are mainly 5 types of jurisdiction which can be classified as follows:

Subject-matter jurisdiction:

It can be defined as the authority vested in a court of law to try and hear cases of a particular type and pertaining to a particular subject matter. For example, District Forums established under the Consumer Protection Act, 1986 have jurisdiction over only consumer-related cases. It cannot try criminal cases.

Territorial jurisdiction:

Under this type of jurisdiction, geographical limits of a court's authority are clearly delineated and specified. It cannot exercise authority beyond that territorial/geographical limit. For example, if a certain offence is committed in Madhya Pradesh, only the courts of law within the boundaries of Madhya Pradesh can try and adjudicate upon the same unless otherwise provided for in a particular piece of legislation.

Pecuniary jurisdiction:

Pecuniary means 'related to money'. Pecuniary jurisdiction tries to address whether a court of law can try cases and suits of the monetory value/amount of the case or suit in question. For example, consumercourts have different pecuniary jurisdictions. A district forum can try cases of value upto Twenty lakh rupees only.

Original jursidiction:

It refers to the authority of a court to take cognizance of cases which can be tried and adjudicated upon in those courts in the first instance itself. It is different from appellate jurisdiction in the sense that in case of the latter, the courts rehear and review an already decided matter whereas in case of the former the cases are tried for the very first time. For example, the High Court of Allahabad has original jurisdiction with respect to matrimonial, testamentary, probate and company matters.

Appellate jurisdiction:

It refers to the authority of a court to rehear or review a case that has already been decided by a lower court. Appellate jurisdiction is generally vested in higher courts. In India, both the High Courts and the Supreme Court have appellate jurisdiction to hear matters which are brought in the form of appeal before them. They can either overrule the judgment of the lower court or uphold it. At times they can also modify the sentence.

Some of the other types of jurisdictions include:

- Concurrent jurisdiction: A situation in which more than one court of law has the jurisdiction to try certain matters. Sometimes, this type of jurisdiction is also referred to as 'co-ordinate jurisdiction'.
- Admirality jurisdiction: Jurisdiction pertaining to mercantile and maritime law and cases.
- Probate jurisdiction: Matters concerning the administration of an estate belonging to a dead person and its guardianship come under probate jurisdiction. For example, cases involving administrationand execution of the will of a deceased person.
- Summary jurisdiction: It refers to the authority of a court to try matters in accordance with the summary procedure. Such cases take form of summary trials in order to speedily resolve a dispute

Indian context of jurisdiction

The original jurisdiction of a court is the power to hear a case for the first time, as opposed to appellate jurisdiction, when a higher court has the power to review a lower court's decision. Original jurisdiction refers to the right of the Supreme court to hear a case for the first time. It has the exclusive right to hear allcases that deal with disputes between states, or between states and the union government. It also has original jurisdiction over cases brought to the court by ordinary people regarding issues to the importance of society at large.

In India, the Supreme Court has original, appellate and advisory jurisdiction. Its exclusive original jurisdiction extends to all cases between the Government of India and the States of India or between Government of India and states on one side and one or more states on other side or cases between different states. Original jurisdiction is related to cases which are directly brought to the Supreme Court. Cases which require the interpretation of the constitution or cases relating to the denial of fundamental rights are heard in the supreme court. In case there is a dispute between two or more states or between the union and the states, the Supreme Court decides such cases. In addition, Article 131 of the Constitution of

India grants original jurisdiction to the Supreme Court on all cases involving the enforcement of fundamental rights of citizens. It is empowered to issue directions, orders or writs, including writs in the nature of habeas corpus, mandamus, prohibition, quo warranto and certiorari to enforce them.

The appellate jurisdiction of the Supreme Court can be invoked by a certificate granted by the High Court concerned under Article 132(1), 133(1) or 134 of the Constitution in respect of any judgement, decree or final order of a High Court in both civil and criminal cases, involving substantial questions of law as to the interpretation of the Indian Constitution.

The Supreme Court has special advisory jurisdiction in matters which may specifically be referred to it by the President of India under Article 143 of the Indian Constitution.

IT ACT 2000

The Government of India enacted The Information Technology Act with some major objectives which are as follows −

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce. The aim was to use replacements of paper-based methods of communication and storage of information.
- To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000. The I. T. Act got the President's assent on June 9, 2000 and it was made effective from October 17, 2000. By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.

Salient Features of I.T Act

The salient features of the I.T Act are as follows −

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that cybercafé is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overridden effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Application of the I.T Act

As per the sub clause (4) of Section 1, nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply −

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A **trust** as defined in section 3 of the Indian Trusts Act, 1882;

- A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Amendments Brought in the I.T Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. It has widened the scope of the term "document" to bring within its ambit electronic documents.
- The second schedule deals with amendments to the India Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.

The third schedule amends the Banker's Books Evidence Act.

International law

Overview

International law consists of rules and principles governing the relations and dealings of nations with each other, as well as the relations between states and individuals, and relationsbetween international organizations.

Public international law concerns itself only with questions of rights between several nations or nations and the citizens or subjects of other nations. In contrast, private international
law deals with controversies between private persons. These controversies arise out of situations which have a significant relationship to multiple nations. In recent years the

line between public and private international law has became increasingly uncertain. Issues of private international law may also implicate issues of public international law, and many matters of private international law have substantial international significance.

Domains of International Law

International Law includes the basic, classic concepts of law in national legal systems (i.e. statutes, property law, tort law, etc). It also includes substantive law, procedural law, due process, and remedies. The following are major substantive fields of international law:

International economic law

International economic law, broadly conceived, is a field of international law that encompasses both the conduct of sovereign states in international economic relations, and the conduct of private parties involved in cross-border economic and business transactions. This includes, among other things, international trade law, law of international financial institutions

International criminal law

International criminal law is a field of international law that seeks to regulate the behavior ofstates, organizations and individuals operating across national boundaries in commission of international crimes. International criminal law also regulates the commission of grave crimes occurring on the territory of sovereign states where those crimes constitute genocide, crimes against humanity, war crimes, or other violations of juscogens norms.

International criminal law is practiced by, and prosecuted within, international criminal tribunals, such as the International Criminal Tribunal for Rwanda, International CriminalCourt and similar courts.

International environmental law

International environmental law (sometimes, international ecological law) is a field of international law regulating the behavior of states and international organizations with respect to the environment. See Phillipe Sands, Principles of International Environmental

Law (2nd ed., Cambridge, 2003). Core domains for international regulation include management of the world's oceans and fisheries, the polar ice caps, and the regulation of carbon and other particulate emissions into the atmosphere

Diplomatic Law

Diplomatic law is a field of international law concerning the practice of diplomacy, and the rights and obligations of state representatives on the territory of other states.

International humanitarian law

International humanitarian law (law of war) is a field of international law regulating armed conflict between states, and more recently, between states and informal groups and individuals. See Jean Pictet, Development and Principles of International Humanitarian Law (1985). International humanitarian law governs both the legality of justifications for war and the legality of wartime conduct international humanitarian law should not be confused
with international human rights law. International humanitarian law is one of the oldest fields of conventional international law. Core principles of international humanitarian law can be found in major international treaties such as the Geneva Conventions of 1949, and thefirst Geneva Convention of 1864.

International Human Rights Law

International human rights law lays down the obligations of Governments to act in certain ways or to refrain from certain acts, in order to promote and protect human rights and fundamental freedoms of individuals or groups. One of the great achievements of the United Nations is the creation of a comprehensive body of human rights law—a universal and internationally protected code to which all nations can subscribe and all people aspire. The United Nations has defined a broad range of internationally accepted rights, including civil, cultural, economic, political and social rights. It has also established mechanisms to promoteand protect these rights and to assist states in carrying out their responsibilities.

Dispute Resolutions

Dispute resolution is a term that refers to a number of processes that can be used to resolve a conflict, dispute or claim. Dispute resolution may also be referred to as alternative dispute resolution, appropriate dispute resolution, or ADR for short.

Dispute resolution processes are alternatives to having a court (state or federal judge or jury) decide the dispute in a trial or other institutions decide the resolution of the case or contract. Dispute resolution processes can be used to resolve any type of dispute including family, neighborhood, employment, business, housing, personal injury, consumer, and environmental disputes.

In addition, the United States Federal Government utilizes dispute resolution processes to assist government employees and private citizens resolve complaints and disputes in manyareas including workplace, employment, and contracting matters.